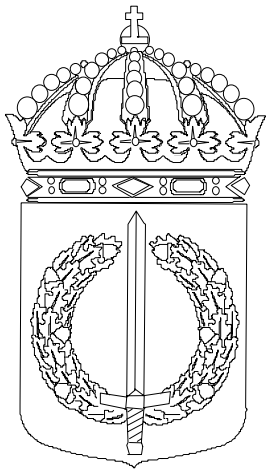
Beteckning

19100:2006

.

Ex ___( )



FÖRSVARSHÖGSKOLAN

Enskild uppsats

Författare	*Förband*	*Kurs*
Mj Roger Nilsson	MarinB S	ChP 00-02
FHS handledare		
Bertil Wennerholm och Fredrik Konnander		
Uppdragsgivare	*Beteckning*	
FHS Krigsvetenskapliga instutitionen	19100:2006	

En svensk ledningsmodell för Informationsoperationer.

Uppsatsen behandlar explorativt en svensk modell för informationsoperationer, avseende ledning och planering, vilken skall kunna verka från nationellt försvar till deltagande i multinationell krishantering.

Syftet med uppsatsen är att bringa kunskap om var Sverige står i dagsläget avseende synen på informationsoperationer som metod, samt ta fram en modell för ledning och planering som passar vårt sätt att leda och planera.

I uppsatsen har en utvecklad kvalitativ metod använts. Metoden har inneburit kvalitativ analys av texter och intervjumaterial. Det vetenskapliga tillvägagångssättet har bestått av analys, framtagande av hypotes, faktainsamling, bearbetning med kvalitativ analys och komparation samt syntes.

Uppsatsen redogör för nuvarande amerikansk och svensk syn på informationsoperationer. Jämför om det finns några avgörande skillnader mellan dessa båda synsätt. Därefter sker en prövning av hypotes som resulterar i en modell, vilken avslutningsvis exemplifieras.

Nyckelord: Informationsoperationer, amerikansk syn, svensk modell, ledning och planering, nationellt försvar .

1. Inledning

1.1 Bakgrund

Mitt intresse för området informationsoperationer har utvecklats, genom reflektioner av händelser i media samt studier av psykologiska operationer under olika konflikter och krig. Ett bestående intryck var bilderna på CNN i oktober 1993. Dessa bilder visade när kropparna, från bland annat besättningen på en nedskjuten Black Hawk helikopter, släpades genom gatorna i Mogadishu av uppretade folkmassor. [1] Effekten av dessa bilder var att den amerikanska hemmaopionen krävde och fick ett utdragande av amerikansk trupp ur Somalia. Händelsen visar på hur asymmetrisk krigföring, förstärkt med media, kan ge ett mycket oväntat resultat. Bruket av media inom ramen för informationsoperationer har, både avsiktligt och oavsiktligt, fått stora konsekvenser under krigen och konflikterna på Balkan. I inledningen av konflikten fick inte ens de grövsta bilder i media det genomslag för krav på ett agerande från världsopionen, som senare ledde till ingripandet i Kosovo. Diverse misslyckade förhandlingsinitiativ, samt inte minst bilder från massakern i Racak den 15-16 januari, [2] fick här NATO att starta ett flygkrig utan FN-mandat.

Under utbildningen vid FHS Taktiska program 1997-98 använde vi den svenska doktrinen, Joint Military Doctrine – Peace Support Operations. I denna berördes informationsoperationer som medel på ett tydligt och markant sätt. Informationsoperationer skall vara en naturlig och integrerad del i alla typer av fredsoperationer. [3] Det som inte berördes var vilka medel som Sverige avser anskaffa eller hur den samordnade ledningen av dessa skulle ske.

Tillbaks på FHS och chefsprogrammet påbörjade vi vår utbildning i operativ planering enligt NATO-modell. [4] Under delkurser i ämnet har det i samtliga

---

[1] Bowden Mark *Black Hawk Down,* som skildrar den amerikanska operationen dagen innan dessa bilder

[2] Annex A till *Lessons from the Crisis*, Ministry of Defence UK, http://www.mod.uk/index.php3?page=1540 , 2001-11-08

[3] FM, *Joint Military Doctrine – Peace Support Operations*, s. 5-4 till 5-6

[4] NATO, *Guidelines For Operational Planning (GOP)*, 1999

fall varit tydligt att informationsoperationer skulle ha verkat som en styrkemultiplikator. Det sätt som debatten i det nu pågående kriget mot terrorism i Afghanistan påverkas av medias rapportering, stärker min uppfattning att informationsoperationer kan vara avgörande för om en militär operation skall lyckas eller misslyckas.

Vilken utveckling har skett i Sverige? Som tidigare nämndes fastställdes redan 1997 avseende deltagande i PSO, att informationsoperationer skall vara en naturlig och integrerad del i lösandet av ställda uppgifter. Utveckling har skett inom arbetsgrupper utsedda av regeringen, [5] samt pågår inom Försvarsmakten. FHS bidrar genom skrivandet av c-uppsatser och begränsade metodförsök vid olika stabsövningar under ledning av CIOS . [6]

[5] Exempelvis Regeringens beslut 12 december 1996 att inom Regeringskansliet tillsätta den så kallade AG IW, efter två propositioner; 1996/97:11 *om beredskapen mot svåra påfrestningar i samhället i fred* och 1996/97:4 *om totalförvaret i förnyelse*

[6] Nationellt centrum för informationsoperationsstudier ingår i Institutionen för Säkerhet och Strategi vid FHS

I de framtidsstudier som förekommer inom ramen för perspektivstudier har man kommit att tala om den fjärde dimensionen i striden. Resultatet av detta syns redan i våra doktrinarbeten; ” *Avgörande för framgång är förmågan att snabbt kunna samla verkan för att hota eller bekämpa motståndaren där denne är sårbar, i mark- sjö- och luft- såväl som i informationsdimensionen. Effektiv samordning av stridens grundelement – bekämpning, rörelse och skydd, liksom stöd i form av logistik och information – är därför nödvändig. Konfliktsituationer där parterna använder andra medel och har andra mål än i traditionella militära konflikter ställer lika höga krav på samordning.* ” [7] Konsekvensen av detta är enligt min mening att även informationsoperationer, som metod, är ett vapen att nyttja tillsammans med övriga stridsmedel för att nå satta mål. Med denna syn på bruket av informationsoperationer har jag valt att skriva uppsats i detta ämne.

1.2 Syfte

Mitt syfte med denna uppsats är att, med hjälp av en explorativ studie, skapa en modell för svensk ledning och planering av informationsoperationer. Fokus på ledningen och planeringen grundar sig på att detta är ett grundfundament för att få önskad effekt av insatser, oavsett vilken av Försvarsmaktens huvuduppgifter det gäller. Vidare har tidigare uppsatser och enskilda utredningar vid FHS inte fokuserat på detta, samtidigt som det nu pågår utarbetande av doktriner på militärstrategisk, operativ samt taktisk nivå inom Försvarsmakten. Från regeringen och Försvarsmakten finns det ett klart och tydligt intresse för hur man kan styra denna typ av operationer. Detta intresse är lätt att förstå med tanke på det informationssamhälle vi nu lever i och de sårbarheter detta bjuder för såväl asymmetrisk krigföring som rena terrorhandlingar.

[7] *FM Grundsyn Ledning*, s. 12.

1.3 Problemformulering

Inom ramen för uppsatsen kommer jag att undersöka hur svensk ledning och planering av informationsoperationer kan ske, oavsett inom vilken huvuduppgift insatsen sker. För att nå dit kommer jag att använda följande huvudfrågeställningar;

- Hur ser den amerikanska doktrinen för informationsoperationer ut?
- Hur ser den svenska Försvarsmakten på informationsoperationer, som metod, över hela konfliktskalan?
- Finns det några avgörande skillnader mellan svensk och amerikansk syn på informationsoperationer?
- Hur skulle svensk planering och ledning av informationsoperationer kunna ske vid försvar mot väpnat angrepp?

1.4 Nyckelord

Ämnesrelaterade tas upp i bilaga 2

1.5 Avgränsningar och antaganden

Uppsatsen inriktas mot ledning och planering inom ramen för en svensk doktrin, detta då jag avser skapa en modell för ledning och planering som täcker hela konfliktskalan. Tidigare c-uppsatser vid FHS gör att jag kommer använda nationellt försvar mot väpnat angrepp som exempel.

Jag kommer endast att i begränsad utsträckning beröra svenska förmågor/medel, då det är en modell för ledning och planering jag avser ta fram.

Som utgångspunkt och referens har jag valt den amerikanska försvarsmakten. Detta motiveras med att amerikanarna är ledande inom metoden. De har redan, i stort, hunnit med att utvärdera sin doktrin ett helt varv genom de erfarenheter som dragits i de senaste konflikterna. Deras arbete sker gemensamt över försvarsgrenarna och det finns omfattande öppet material om hur detta skett.

NATO hade varit en naturlig referens med anledning av vårt medlemskap i PFF, men föll på att deras doktrin är ”Restricted” och då hemligstämplad i Sverige.

Källor och material som är hemliga har ej använts i uppsatsen. Det är FHS uttalade inriktning att enbart använda öppna arbeten och källor.

Uppsatsen bygger på ett avgörande antagande, nämligen att en fortsatt svensk anpassning av operativ planering sker mot NATO:s modell. Motiven är dels att det är den modell som används vid FHS samt pågående arbeten inom Försvarsmakten. [8] Detta antagande gör det möjligt att ta fram en och samma modell för såväl nationellt som internationellt användande av informationsoperationer.

[8] Ibid. s. 23.

1.6 Teorianknytning

Valet av teorianknytning har varit svårt eftersom uppsatsen är explorativ inom ett till sin art tämligen diffust ämne Ledning, vilket i sig innebär att det jag tar fram kan ses som en teori. Efter diskussion med min handledare, och med Anders Johansson, [9] bestämde jag mig för att använda mig av kombinationen ”bevisets väg” [10] och John Kingdons teori om agendor. [11]

I samband med min kunskapsuppbyggnad, i form av bokstudier, fann jag en teori som Martin van Creveld använt vid studier av ledning och dess utveckling i boken ”Command in War”. Martin van Creveld är en internationellt erkänd militärhistoriker och författare som bland annat undervisat historia vid Hebrew University i Jerusalem, men även har en militär bakgrund i den israeliska försvarsmakten. I boken studerar van Creveld utvecklingen av ledning ur ett historiskt perspektiv. Den enligt honom själv viktigaste slutsatsen är: det har inte funnits eller finns en teknisk lösning som klarar att undanröja krigets osäkerhet. Valet är fortfarande mellan centraliserad eller decentraliserad ledning eller att kombinera dessa. För att kunna studera utvecklingen klassificerar van Creveld ledning (command) genom att dela in funktionen i tre huvudkomponenter; 1) organisation, 2) procedurer och metoder samt 3) tekniska hjälpmedel. [12] Hans ansats är att ledning i grunden är en process, som använder information för att koordinera människor och ting till att utföra ett uppdrag med en gemensam målsättning. [13] Jag valde då att gå vidare med en begränsad form av detta teoretiska synsätt på ledning, eftersom jag delar van

---

[9] Johansson arbetar vid Instutitionen för Säkerhet och Strategi vid FHS. Han har god erfarenhet av att skriva c-uppsatser samt även tidigare varit handledare. Johansson har också goda kunskaper och praktisk erfarenhet från Bosnien avseende användandet av informationsoperationer.

[10] Starrin et.al

[11] Teorin har använts av Ulf Kurkiewicz i dennes uppsats *Informationsteknologins inverkan på svensk försvarspolitik*, FHS beteckning 19100:6010

[12] van Creveld, s. 9-10

[13] Ibid. s. 263

Creveld övergripande syn på ledning i denna bok. Den förändring jag gjorde var att endast använda två av de tre komponenterna i mitt arbete, organisation samt procedurer och metoder. Mitt motiv för att ta bort tekniska hjälpmedel har en praktisk, men också en filosofisk aspekt. Praktiskt fanns risken för en splittring av fokus, på grund av tid och utrymme, från kärnan av ledning genom att även se till den tredje faktorn. Filosofiskt innebär en tidig syn på tekniken en form av begränsning, eftersom det i grunden handlar om en mänsklig tankeprocess inom ramen för kampen mellan minst två olika viljor. I min analys kommer jag att dela på van Creveld andra komponent, procedurer och metoder, och använda komponenterna med följande innebörd. Organisation; sättet vilket staber är indelade, Procedurer; de processer som förekommer inom staben för att kunna lösa ställda uppgifter samt Metoder; hur organisationen arbetar i processerna.

Vad är egentligen den svenska Försvarsmaktens vilja avseende informationsoperationer? Denna kompletterande fråga uppstod med tanke på en av huvudfrågorna i uppsatsen; Hur ser den svenska Försvarsmakten på informationsoperationer, som metod, över hela konfliktskalan? Efter att ha läst officiella tryck och uttalanden, från såväl politisk som militär sida, uppfattade jag en diskrepans mellan ord och handling. För att kunna analysera denna fråga kommer jag att använda John Kingdons teori om agendor. [14] Kingdons teori grundar sig på antagandet att det går att förstå beslutsprocessen genom att studera de ingående aktörerna och de politiska processerna som försiggår inför ett politiskt beslut. Både processen och aktörerna kan påverka beslutsagendan och på så sätt påverka vilka områden som leder till beslut och vilka som läggs åt sidan. Enligt Kingdon är det fyra processer som inverkar på den politiska agendan;

- De existerande problemområdena
- De olika förekommande policyflödena
- Gällande politiska realiteter, exempelvis, partipolitik

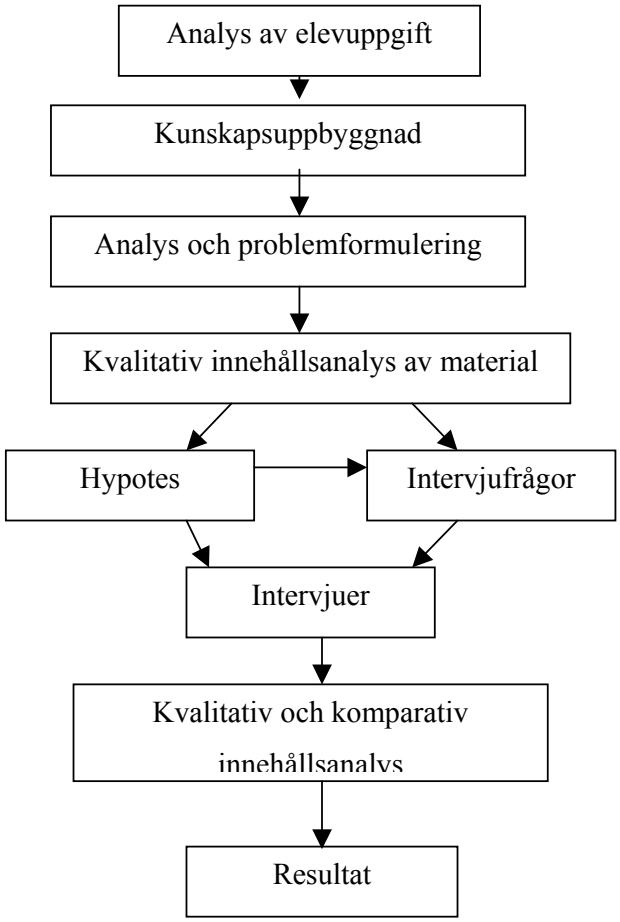
[14] Kingdon, s.16-18

- Tillgängliga problemlösningar som inte är allmänt kända

Jag finner att det går att använda denna teori för min kompletterande frågeställning, eftersom denna berör en iterativ process. Utvecklingen av informationsoperationer som metod inom Försvarsmakten startas av regeringen, förädlas inom försvarsmakten och återrapporteras till regeringen. Under denna process utvecklas och berörs även de av Kingdon angivna fyra processerna. För att skapa ett underlag för analys har jag utformat frågeställningarna för intervjuerna enligt bilaga 3.

1.7 Metodbeskrivning och disposition

Hur undersöker man någonting på ett vetenskapligt sätt? I min uppsats söker jag något som vi idag saknar inom Försvarsmakten, vilken metod passar då bäst i den flora som finns? Jag valde att låta min problemformulering bli utgångspunkten, vilket ledde till en utvecklad kvalitativ metod enligt översiktsbilden nedan.



Första steget i processen var att analysera själva uppgiften, att skriva en c-uppsats inom ett fritt valt ämnesområde. Några enkla riktlinjer följde denna uppgift. Jag fastnade för två budskap; passa på att lära er något nytt och se om uppsatsen kan bibringa något till utvecklingen av Försvarsmakten. Jag kom snabbt fram till ämnet informationsoperationer, som är helt nytt för mig och under utveckling inom Försvarsmakten. Fasen med kunskapsuppbyggnad kom att i huvudsak bli tvådelad, dels teoretiskt genom böcker och ett par enskilda föreläsningar, samt rent praktiskt genom att gå övad i funktionen under två stora stabsövningar vid FHS. Efter detta genomförde jag en analys och problemformulering av ämnet för min uppsats, vilken ledde till en kvalitativ innehållsanalys av litteratur och anteckningar från såväl övningar som föreläsningar. Jag skapade mig en hypotes för svensk ledning och planering av informationsoperationer: nuvarande amerikansk modell är direkt applicerbar för svenska förhållanden. En kompletterande fråga blev det något överraskande resultatet av denna fas, nämligen diskrepansen mellan nedtecknat budskap och praktiska åtgärder i Sverige. Detta föranledde behovet av intervju i min studie. Jag valde i samråd med handledaren ut ett antal nyckelpersoner inom och utom Försvarsmakten, som bedömdes kunna såväl besvara den kompletterande frågan som ge relevant underlag för analysdelen av uppsatsen. Jag kom främst av tidsskäl att enbart genomföra intervju med två personer, genom sina roller på militärstrategisk och operativ nivå svarar de för de mest styrande nivåerna för min uppsats. Intervjuerna genomfördes på personernas ordinarie tjänsterum och dokumenterades genom anteckningar av mig. Direkt efter genomförd intervju renskrev jag sedan svaren på mina frågeställningar. Efter genomförda intervjuer var det dags för den avgörande kvalitativa och komparativa analysen av inhämtat underlag. Sett mot såväl hypotes som den kompletterande frågeställningen, denna analys resulterade i en modell för svensk ledning och planering. För att exemplifiera denna valde jag ett scenario, i huvudsak från Idébild A,[15] för nationellt försvar mot väpnat angrepp.

[15] *Försvarsmaktsidé och målbild Rapport 5*, s. 135

Min valda metod har gjort att jag disponerar uppsatsen enligt följande. Först ett inledande kapitel som beskriver hur jag kom fram till detta ämne och problem, vald metod och teori samt en enklare granskning av källmaterialet. Därefter ett kapitel som kortfattat beskriver den amerikanska doktrinen för informationsoperationer, vilket syftar till att ge läsaren en förståelse för denna och samtidigt ge svaret på min första frågeställning. Nästa kapitel beskriver svensk syn på informationsoperationer. Här kommer en redogörelse för såväl skrivna som muntliga påståenden från Försvarsmakten. Det fjärde kapitlet, och tillika uppsatsens tyngdpunkt, är en komparativ jämförelse och analys mellan amerikansk och svensk syn på främst ledning och planering. I femte kapitlet prövas framtagen hypotes, vilket leder till det sjätte kapitlet. Här presenteras och exemplifieras framtagen modell för svensk ledning och planering av informationsoperationer samt ges rekommendationer av fortsatta studier inom området. Uppsatsen avslutas med en sammanfattning.

1.8 Kommentarer kring källmaterialet

Huvuddelen av mitt källmaterial är officiella tryck vilket medger en säker källkritisk granskning. Urvalet av relevant litteratur och annat tryck har skett i samråd med handledare och överstelöjtnant Johan Lindberg vid CIOS.

Det underlag som jag hämtat från internet är taget från enbart officiella hemsidor och främst från olika myndigheter. Detta ökar tillförlitligheten och kan antas vara respektive organisations offentliga ställningstagande. I den mån det varit möjligt har jag även kontrollerat min uppsats centrala delar mot andra källor i Sverige.

Eftersom uppsatsen är av explorativ art har jag valt att ta med material som är under utveckling, exempelvis utkastet till svensk militärstrategisk doktrin. Man kan förvänta sig att huvudbudskapen inte kommer att ändras, utan ändringar är mer av språklig och redaktionell art.

1.9 Forskningsläget

Vid FHS har det under de sista tre åren skrivits en enskild utredning och två uppsatser inom ämnet informationsoperationer. Utav dessa verk så är det den enskilda utredningen ”Informationsoperationer, En möjlighet för Sverige?” av major Anders Frykholm [16] som har tydligast beröring med mitt ämne. Detta då Frykholm tar upp ledning och planering, men med en annan angreppsvinkel och jämfört med svensk operativ bedömandemall. Detta gör att jag inte finner det lämpligt att jämföra mina resultat med Frykholms. De andra två uppsatserna är ”Informationsteknologins inverkan på svensk försvarspolitik” av major Ulf Kurkiewicz, [17] vilken inte ser specifikt på informationsoperationer som metod samt ”Informationsoperationer vid fredsfrämjande insatser – svensk förmåga eller oförmåga?” av major Per Klingvall. [18] Denna uppsats behandlar främst förmågor vid en enskild typ av insatser. För att visa på bredden av intresse för informationsoperationer kan nämnas att det även på civila universitet skrivs uppsatser inom området. Exempelvis ”Psykologiska Operationer – strategisk kommunikation som brottsbekämpare”? av Petter Larsson; Sociologiska Instutitionen, Avdelningen för Medie- och Kommunikationsvetenskap vid Lunds universitet.

Inom Försvarsmakten finns det på Högkvarteret ett par personer som inom ramen för projektet Ny krigföring, ser på utvecklingen av informationsoperationer. Nyligen har det också tagits beslut att vid Operativa insatsledningen tillsätta en speciell befattningshavare för området informationsoperationer. [19] Generellt kan sägas att dessa båda arbeten kommit så långt att det finns utkast på definition av begrepp och termer inom metoden och allmänna formuleringar kring utformningen av ledning och planering. De framlagda förslagen på definitioner återfinns i bilaga 2 samt till del i kapitel 3 och 4.

---

[16] FHS beteckning 19100:6021, 2000

[17] FHS beteckning 19100:6010, 2000

[18] FHS beteckning 19100:1002, 2001

[19] Enligt uppgift från major Per Klingvall, C Info vid Operativa insatsledningen

2. Hur ser den amerikanska doktrinen för informationsoperationer ut?

2.1 Allmänt

Underlaget för detta kapitel kommer främst ur två amerikanska publikationer, ”Joint Pub 3-13 Joint Doctrine for Information Operations” utgiven den 9 oktober 1998 samt utkastet till ”Marine Corps Warfighting Publication (MCWP) 3-36 Information Operations” daterat den 27 februari 2001. Motivet till användandet av dessa båda är att den förstnämnda är grunddokumentet inom den amerikanska försvarsmakten och med den som grund har respektive försvarsgren utarbetat sina egna. USMC är, enligt min uppfattning, en bra utgångspunkt för jämförelse för en liten nation som Sverige. USMC arbetar med ”Marine Air-Ground Task Force” regelbundet på såväl operativ som taktisk nivå. Detta innebär att kåren innehåller förutom egna markstridskrafter och underhållsförband även egna flygstridskrafter som bildar tillfälligt sammansatta stridsgrupper för att lösa en uppgift. Resurserna som disponeras för detta stämmer bättre för en jämförelse med svensk försvarsmakt än stormakten USA:s samlade stridskrafter. USMC är också den amerikanska försvarsgren som mest liknar den svenska försvarsmakten och vårt sätt att arbeta med manövertänkande och ledning genom uppdragstaktik.

Den amerikanska synen på informationsoperationer grundar sig i huvudsak på följande faktorer; den teknologiska utvecklingen, nya aktörer och motparter samt ändrade uppgifter för försvarsmakten. Budskapen i dessa är att vi idag lever i en föränderlig värld där det är mycket svårt att förutsäga vilken motpart man kommer att möta, allt från nationalstater till enskilda individer och organisationer med mer eller mindre klara syften. Informationsteknikens utveckling har skapat nya möjligheter och begränsningar för att såväl agera som att bli utsatt för olika former av angrepp, där man med enkla medel kan få stora effekter utan att direkt röja sig själv. Dessa saker har gjort att vi idag spelar över hela konfliktskalan på ett mycket bredare och varierande sätt än tidigare. För amerikanska försvarsmakten har konsekvensen blivit att de mer

och mer löser andra uppgifter än de direkta krigsmässiga och detta ställer ett ökat krav på förmågan att hantera informationsoperationer.

Sammanfattningsvis ser amerikanarna informationsoperationer som åtgärder för att påverka motståndarens information och informationssystem, samt skyddet av egna. Dessa är kritiska faktorer för en ”joint force commander`s” förmåga att uppnå och bibehålla informationsöverlägsenhet, vilket man anser är förutsättningen för avgörande ”joint operations”. [20]

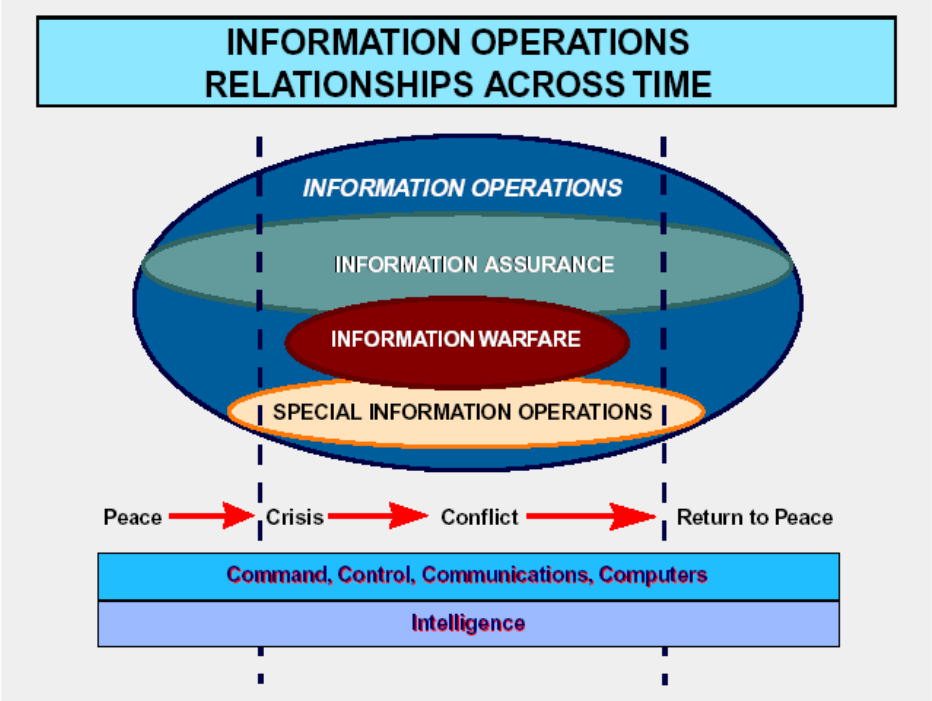


Figure I-2. Information Operations Relationships Across Time

Bilden är tagen ur Joint Pub 3-13 sidan I-4 och beskriver den amerikanska synen på förhållandet mellan informationsoperationer och tidsskalan för olika konfliktnivåer.
Enligt den amerikanska synen ger informationsoperationer bäst effekt i fred eller början av en kris/konflikt då man har stora möjligheter att förhindra en eskalering eller helt lyckas stoppa en kris/konflikt. Om man inte hinner upptäcka och agera i dessa faser ger metoden ökade möjligheter att trappa ned

[20] *Joint Pub 3-13* s. vii

en konflikt i kombination med andra tillgängliga medel. Under konflikter trycker man på vikten av att samordna informationskrigföring för att få bästa möjliga effekt av tillgängliga politiska, ekonomiska och militära medel, i en konflikt eller kris benämner man informationsoperationer detta. Amerikansk syn på huvudsyftet med informationsoperationer över de olika konfliktnivåerna sammanfattas enligt följande: I fred ”influence”, före eller i starten av en kris ”deter”, under krisen ”enable” samt efter krisen ”restore”. Dessa syften används även när man talar om det traditionella kriget. En liten varning för dessa syften. Det går inte att direkt översätta dessa till svenska för en enkel förklaring. I den amerikanska synen har dessa syften en variation avseende innebörd, beroende på läget och medel. För att förstå den mer exakta innebörden måste man alltså alltid sätta syftet i sitt sammanhang.

Från amerikansk sida har man satsat mycket resurser på att utveckla och bli ledande inom informationsoperationer, detta då effekten av en händelse på lägsta nivå, med hjälp av informationstekniken, mycket snabbt kan ge verkningar på högsta politiska nivån.

2.2 Definitioner och omfattning av informationsoperationer

Följande definition av informationsoperationer är gällande; ”Actions taken to affect adversary information and information systems while defending one’s own information and information systems. Also called IO. (This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)” [21]

Följande bild visar förmågor och angränsande områden som innefattas av amerikanska informationsoperationer.[22]

[21] Ibid. s. GL-7

[22] Ibid. s. I-10

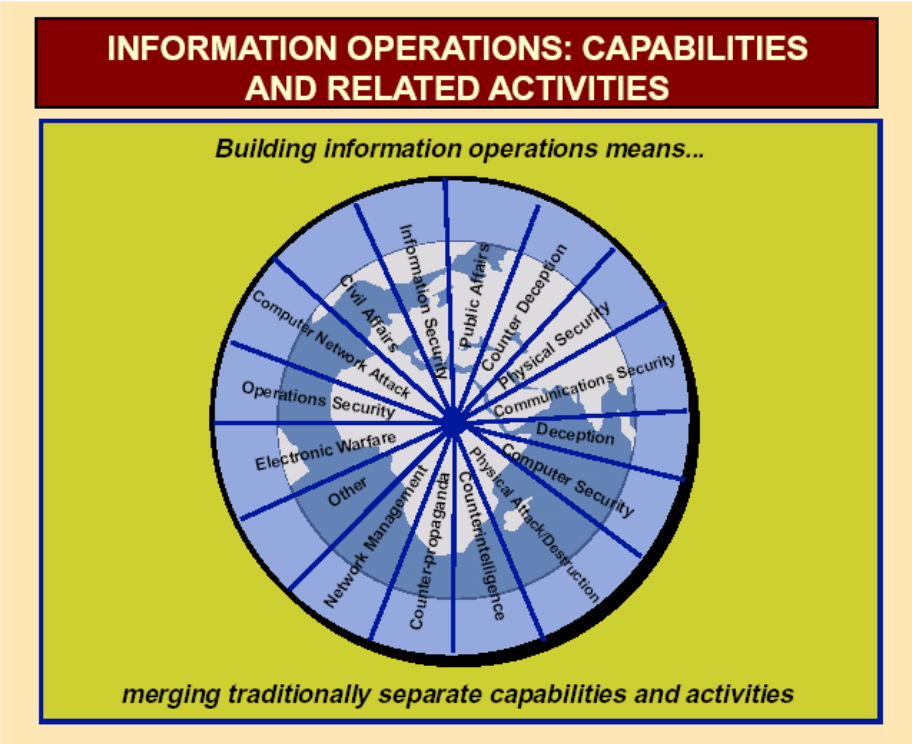
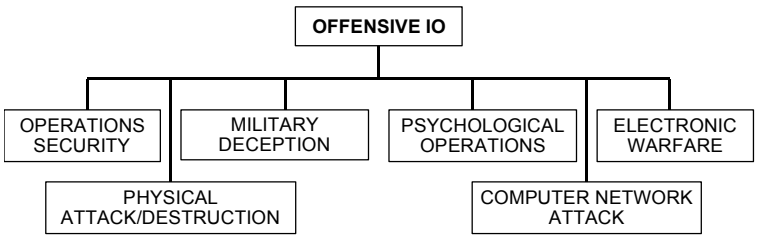


Figure I-3. Informations Operations: Capabilities and Related Activities

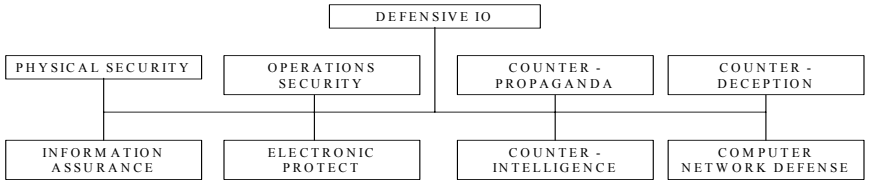
Informationsoperationer i sin tur delas i in två huvudgrupper som benämns ”offensive” samt ”defensive”. Följande förmågor, eller komponenter, ingår i respektive: [23]



Det yttersta målet med offensiva informationsoperationer är att påverka motpartens beslutsfattning genom dennes, eller dessas, informations- och beslutsstöd. Detta kräver samordnade insatser baserade på underrättelser av i bilden angivna förmågor. Denna indelning skall inte ses som statisk eller gjuten

[23] *MCWP draft 3-36*

i cement, det kan även tillkomma andra förmågor inklusive användandet av defensiva informationsoperationer som en del i det offensiva. Man poängterar vikten av att mål och syfte med vidtagna åtgärder är samordnade från strategisk till taktisk nivå, samt att man hela tiden kommer ihåg att det inte är några skarpa och tydliga gränser mellan dessa. Avseende ”computer network attack” påpekas också att denna förmåga med stor sannolikhet inte finns på taktisk nivå, eller i operationsområdet, utan är baserad hemma i USA. Effekterna fås ändå där de så önskas då denna attack i första hand sker över det globala nätverket. Vid användandet av offensiva informationsoperationer trycker man på de lagliga aspekter som finns att ta hänsyn till, samt att effekten av vissa insatser är mycket svårt att förutsäga.



Vid planeringen och användandet av defensiva informationsoperationer ställs särskilda krav på att analysera och bedöma sina egna systems sårbarheter. Det är inte bara en fråga om olika typer av skyddsåtgärder utan här innefattas även policys, människor och vissa processer:

- Skyddet av informationsmiljön innebärande hela skalan från egna informationsbehov till hur vi delges och bearbetar denna. Denna process är alltså en kombination av råvara, tekniska system och anläggningar samt människan i systemet.
- Förmågan att upptäcka en attack från en motpart, mot ledningssystem och sensorer på fältet. Dagens framgrupperade enheter är mer eller mindre beroende av det globala nätverket, förmågan att detektera och

identifiera attacker över detta ställer stora krav på hård- och mjukvara. Den amerikanska lösningen är att denna typ av övervakning och skydd sker från USA med gemensamma resurser.

- Förmågan att snabbt återställa eller hitta nya vägar efter, exempelvis, en nätverksattack för ett ledningssystem.
- Förmågan till motattack, vilket är en komplex och svår process att hantera. Tidig och säker identifiering anser amerikanarna vara väsentlig i denna fråga, på vilket sätt och med vilka medel man sedan genomför motattacken kan skifta från vapenmakt till en politisk protestnot.

Vilka typer av mål amerikanarna ser för informationsoperationer framgår av bilden nedan. [24]

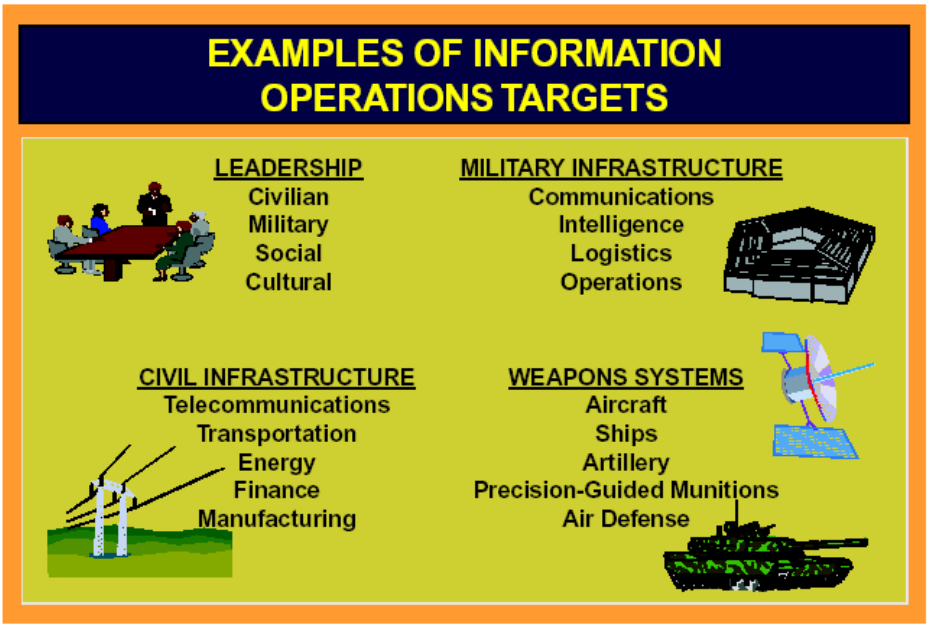


Figure I-8. Examples of Information Operations Targets

2.3 Ledning och planering

Det är amerikansk syn att informationsoperationer bedrivs på samtliga nivåer under en konflikt eller krig, varvid mål och metoder kan variera beroende på nivå. Gränssnittet mellan nivåerna kommer inte att vara tydliga och klara utan

[24] *Joint Pub 3-13* s. I-17

kräver en förståelse för interaktionen mellan dessa. Följande tre övergripande nivåer bör klaras ut för att säkerställa optimal effekt av insatserna:

1. Strategisk nivå klarar ut nationella målsättningar för alla typer av medel från politiska till militära. Detta kommer att kräva en omfattande koordinering och samordning mellan Försvarsmakten andra nationella, multinationella, myndigheter och organisationer. Detta ansvarar den politiska ledningen för, i Sverige kallad nationell strategisk nivå. [25]

2. På operativ nivå genomförs informationsoperationer för att uppnå eller understödja kampanj eller operativa mål. Fokuseringen på denna nivå kommer normalt att vara mot motpartens ”lines of communications”, logistik och förmågan till ”command and control”. Det övergripande syftet är att begränsa motståndarens förmåga till beslutsfattning och manöver. Detta skapar förutsättningar för upprättande, samt bibehållande av, informationsöverlägsenhet vilket leder till avgörande i operationen.

3. Den taktiska nivån strävar efter att uppnå specifika taktiska mål. Huvudfokus här är att påverka eller slå mot motståndarens informations- och ledningssystem. Här påtalas vikten av att vid planeringen och ”targeting-processen” inte glömma att dessa system består av människor, tekniska system, information och metoder. Samtidigt som offensiva åtgärder vidtas mot motståndaren måste även defensiva åtgärder vidtas för att skydda egna motsvarande system.

Amerikanarna talar om skillnaderna mellan planering i förhand (deliberate planning) och planering under tidspress eller efterhand (crisis action planning). De avgörande skillnaderna är konsekvenserna av tidsfaktorn och metodiken i planeringen. Vid planering i förhand finns tiden för noggrann och detaljerad underrättelseinhämtning samt att de olika, i fred organiserade, befälhavarna

[25] *FM Grundsyn ledning*, figur s. 17

känner och agerar i området. Vid planering i efterhand utses normalt en ”joint force commander” som påbörjar sin planering under tiden som styrkan organiseras, konsekvensen blir att vikten av parallell planering ökar samt att noggrannheten i underrättelserna nedgår. Det sistnämnda omnämns särskilt eftersom detaljerade och aktuella underrättelser är mycket väsentligt för att få rätt effekt av, exempelvis, psykologiska operationer. Bilden nedan sammanfattar metoden för detta.[26]

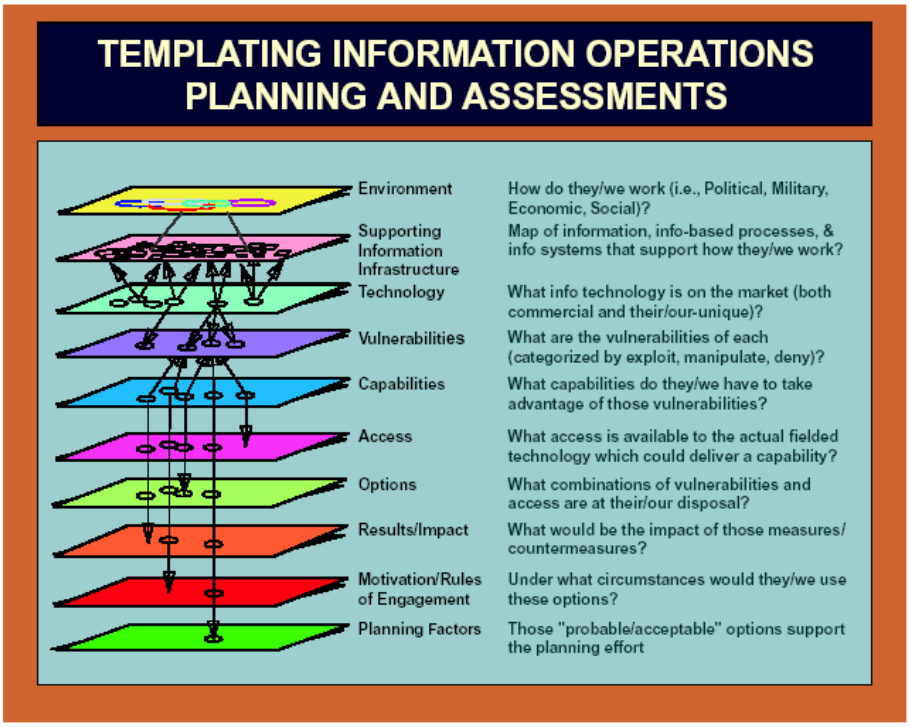


Figure V-2. Templating Information Operations Planning and Assessments

Framgångskriterier för att få en bra planering uttrycker amerikanerna enligt följande:

- Hög förståelse för integrering av informationsoperationer med övriga militära medel krävs.
- Fokusera på syfte och målsättningar, dessa fås ur högre chefs och egen chefs beslut i stort och operativ idé.
- Vikten av synkroniserade syften och målsättningar mellan de olika nivåerna samt mellan de olika ingående styrkekomponenterna.

---

[26] *Joint Pub 3-13* s. V-4

- Samordningen av, till informationsoperationer angränsande områden, och åtgärder för att få synergieffekt och undvika kontraproduktiva effekter.
- Vikten av underrättelser under planering, genomförande och uppföljning av informationsoperationer samt att det är svårt att finna tydliga sätt att genomföra verkans- och effektbedömningar.

Hur organiserar då amerikanarna sig när det gäller planering, genomförande och uppföljning av informationsoperationer? [27]

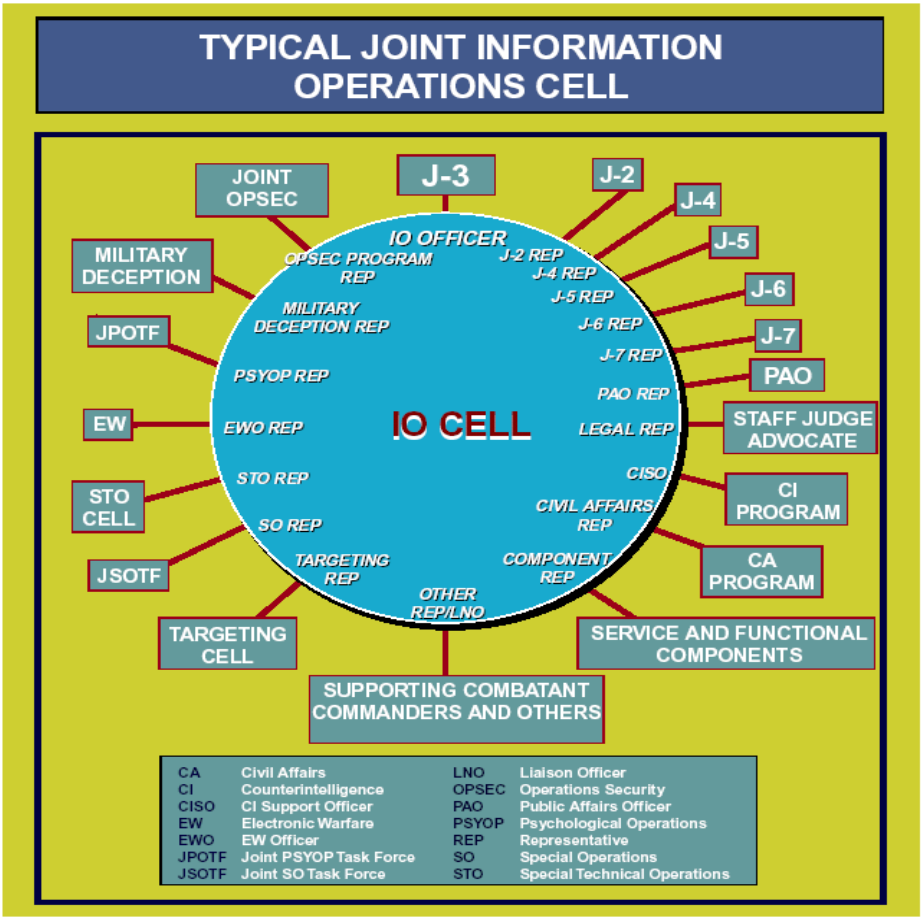


Figure IV-1. Typical Joint Information Operations Cell

Denna bild visar på principen för en så kallad IO-cell. IO-cell används i stort sett på samtliga nivåer inom den amerikanska försvarsmakten. Den har tidigare benämnts, och benämns fortfarande ibland inom armén, för ”IO battle staff”.

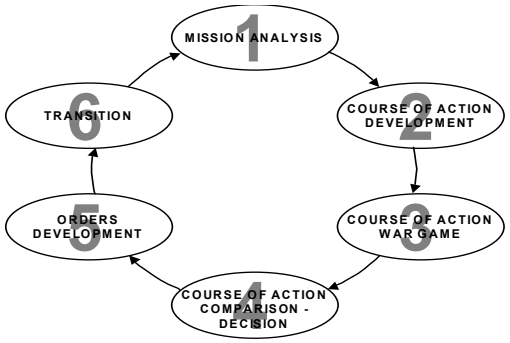
[27] Ibid. s. IV-3

Huvudprincipen är att den verkar intermittent: deltagarna samlas under vissa perioder under planering, genomförande och uppföljning av en operation eller insats. Ansvaret för att kalla samman och leda arbetet ligger normalt på J3 ”Operations”. Motivet till detta är att säkerställa synergieffekten av alla olika tillgängliga medel. IO-cellen är mekanismen för samordning av alla ingående och angränsande resurser. Under planeringen ska IO-cellen samordna mellan alla i styrkan ingående komponenter, med sidoordnade förband, med högre chef och med eventuella andra understödjande myndigheter eller organisationer. I genomförande och uppföljning skall cellen vara beredd att genomföra uppkommen samordning, ändring av prioriteringar av mål samt eventuella förändringar i syften. Detta kräver att cellen över tiden antingen finns i direkt anslutning till ledningscentralen eller har samband till densamma.

För att underlätta genomförande och uppföljning används ”Information Operations Work Group (IO WG)”. Denna grupp är en förlängning av IO-cellen och samlas vid särskild tid och plats för att främst underlätta arbetet vid ”Joint Coordination Targeting Board (JCTB)”. (Deltagarna är situationsberoende) Vad som är av särskild vikt är att ”IO WG” arbetar med samma tidshorisont som övriga i ”targeting-processen” nämligen 24h, 48h och 72h. Samling av ”IO WG” bör ske innan ”JCTB”, men måste ske före de dagliga pressbriefingarna. Detta för att effekten av perceptionsstyrning inte skall gå förlorad eller motarbetas av egna uttalanden.

Vilka processer och metoder finns det inom staben som IO-cellen bör medverka i för att säkerställa effekten av informationsoperationer? Dessa är olika planeringsgrupper, genomförande verksamheten (current operations) och bekämpningsledningen (targeting staff). Vikten av insyn och medverkan i bekämpningsledningen kan inte nog understrykas, enligt amerikanarna. Är inte åtgärderna för målbekämpning och informationsoperationer synkroniserade eller samordnade kommer inte informationsoperationer att stödja den pågående operationen eller insatsen.

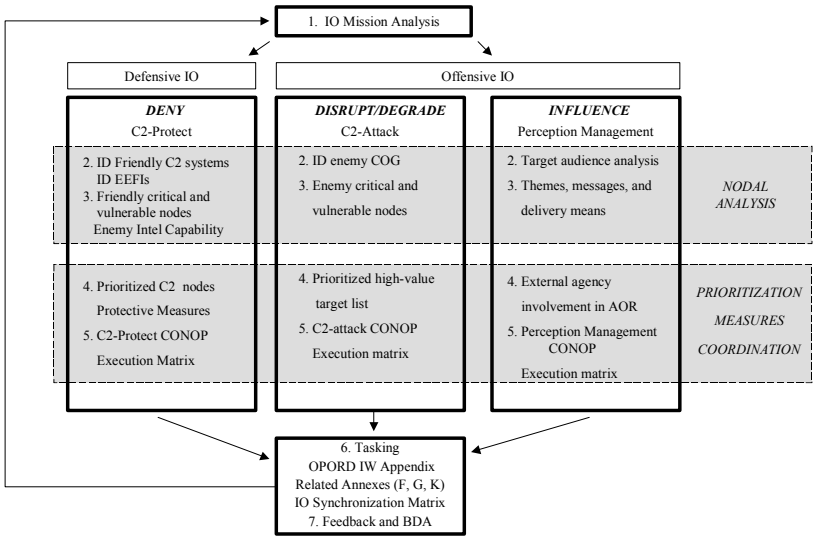
För att exemplifiera hur den operativa planeringen kan gå till kommer här en kort sammanfattning på amerikanska marinkårens planering och genomförande process. Följande planeringsmodell används:



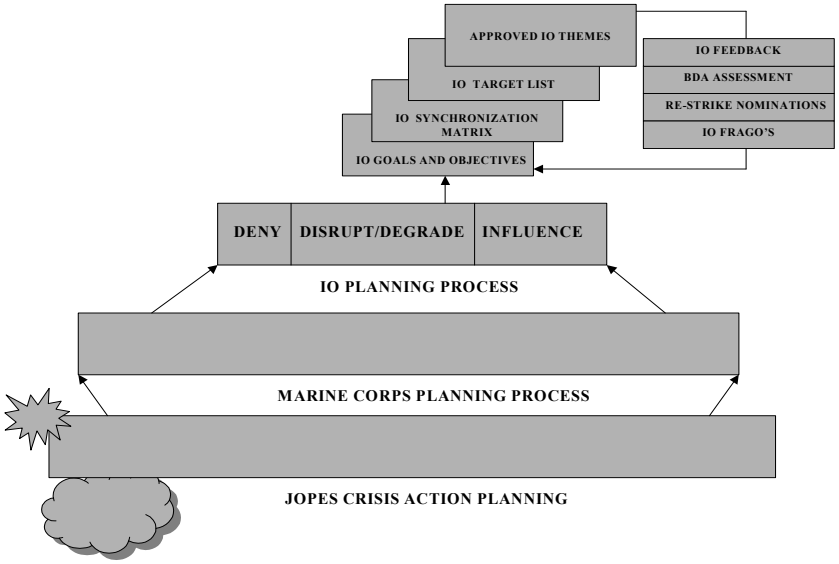
Modellen utgår från befälhavarens centrala roll i beslutsfattningen. Den fokuserar på uppgiften och aktuell hotbild samt strävar efter kraftsamling av effekt samt understödjer skapandet och bibehållandet av tempo. Vid planeringen använder man sig av följande funktioner för att säkerställa integrerad och parallell planering; ”command and control, maneuver, fires, intelligence, logistic and force protection”. [28]

[28] *MCWP draft 3-36*

Följande bild visar på hur bedömandet av informationsoperationer sker inom ramen för denna planeringsmodell.



Det är viktigt att komma ihåg att det alltid pågår såväl offensiva som defensiva åtgärder. I bedömandet söker man kritiska sårbarheter efter angivna strategiska och operativa ”centers of gravity”, dessa säkerställs sedan genom att understödja de framtagna handlingsalternativen.
Under operationens genomförande sker fortlöpande utvärdering av informationsoperationer enligt bilden.



De viktiga verktygen, i denna process, för att styra genomförande och uppföljning är;

- fastställda syften och mål
- IO synkroniseringsmatris
- IO målvalslista
- Godkända och fastställda meddelanden och teman för perceptionspåverkan.

2.4 Viktiga erfarenheter från genomförda operationer

Den amerikanska försvarsmakten har efter genomförda operationer och övningar dragit och dokumenterat erfarenheter om användandet av informationsoperationer. En särskild cell vid Center for Army Lessons Learned (CALL) i Fort Leavenworth Kansas har sedan utvärderat dessa erfarenheter så att de har kunnat användas i utvecklingen av IO. [29]

Då de flesta operationer, där informationsoperationer använts, varit olika ”Peace Support Operations (PSO)”, (PSO är en del av det amerikanarna benämner ”Military Operations Other Than War (MOOTW)”), trycker CALL på vikten av att använda hela spektret inom metoden som ett medel. Möjligheten att med offensiva informationsoperationer direkt påverka motpartens förmåga att fatta beslut och leda, eller till och med direkt påverka dennes ”center of gravity” lyfts fram. Denna möjlighet gäller över hela konfliktskalan och bör inte förringas. [30] För att detta skall fungera och säkerställas tar man upp ett antal faktorer kring ledning och planering som gäller från operativ ned till stridsteknisk nivå. Fokuseringen av informationsoperationer återfinns i chefens beslut i stort. I dessa måste tidpunkter och eventuella platser framgå där han/hon vill ha optimal effekt av alla sina tillgängliga medel, inklusive informationsoperationer. För att säkerställa att så sker bör därför chefen vara med, om inte hela tiden så åtminstone vid uppstarten av, ”JCTB” eller IO-synkroniseringsmötet inom IO-cellen. Här får chefen kunskap om effekter av genomförda samt kommande informationsoperationsinsatser och kan direkt besluta om eventuella ändringar i prioriteringar eller annat.

---

[29] Resultatet av dessa går att läsa på länken *http://call.army.mil/call.html*

[30] Mr Roy W. Hollis *Information Operations Observations, TTP, and Lessons Learned*.

Bildandet av IO-cell och utbildning samt övning av densamma bör ske redan vid hemmaförbandet för att säkerställa effektiviteten vid insats. Exakt utformning och rutiner ska vara uppgiftsberoende. [31]

Angående planering och genomförande påpekas följande viktiga erfarenheter; Först måste staben och chefen ha förståelse för de skillnader som finns mellan informationsoperationer och traditionella medel. I amerikanska armén har ordinarie stridsuppgifter olika betydelse, skillnaden måste vara klar. Exempel:

CONVENTIONAL	OBJECTIVE	INFORMATION OPERATIONS
Reduce Options of Courses of Action	LIMIT	Minimize Influence
Preclude Effectiveness	DISRUPT	Reduce Effectiveness
Alter Time of Arrival	DELAY	Hinder Decisionmaking

Bilden skall läsas genom att först se till ”objective” och sedan se på förklaringen av innebörden för respektive medel.

Vidare måste det finnas en tydlig förståelse för svårigheten med verkansbedömning och tidsaspekten för denna. När sedan stabens olika delar arbetar tillsammans i planeringsgrupper eller vid olika stabsmöten, måste man på ett tydligt sätt visa informationsoperationsinsatserna. Ett sätt att göra detta är att använda samma typer av tabeller och matriser, främst J2 och J3, modifierade så att de passar informationsoperationer. [32]

Från insatserna i Bosnien tas följande viktiga erfarenheter upp: Vid en PSO är inte de tidigare parterna våra motståndare, utan den egentliga motståndaren är orsaken till konflikten. Detta påverkar främst vilka förmågor som kan användas, men medger ofta bättre möjligheter att med informationsoperationer påverka ”center of gravity”. För att kompensera begränsningen av vissa förmågor krävs ett asymmetriskt tänkande gällande såväl metoder och

[31] Ibid.

[32] Maj Matt Andersson mfl *Battalion/Task Force Targeting and the Military Decision-Making Process (MDMP) in the Information Operations (IO) Environment*

processer som organisation. Det finns från Bosnien gott om exempel på detta på såväl divisions som bataljonsnivån. Exempel finns på hur bataljoner har använt lokala radiostationer för att minimera risken för en eskalering av spänningen vid olika former av tillslag, men man poängterar vikten av att de teman och meddelanden som används måste vara sanktionerade och ensade så att man talar med en röst inom hela styrkan. Planering och ledning av informationsoperationer tas också upp där man varnar för olika syn och regelverk mellan deltagande nationer. Dessa skillnader kan användas som en styrka men bara man är medveten om att de existerar annars kan detta snabbt bli en svaghet. [33]

2.5 Slutsatser

Informationsoperationer är i sig inget nytt. Det som är nytt är helhetsgreppet man tagit genom användandet av informationsoperationer som metod. Tidigare har ingående förmågor och angränsande områden använts separat utan någon tydlig samordning. Helhetsgreppet säkerställer att metoden går att använda för att få synergieffekter med övriga tillgängliga medel för den militäre chefen.

För att få optimal effekt av informationsoperationer krävs detaljerade och noggranna underrättelser, vilket kräver ett långt och tålmodigt arbete. Detta arbete bör genomföras redan under fred och inom troliga krisområden samt främst inriktas mot underlag för perceptionspåverkan. Effektbedömning av gjorda insatser ställer också stora krav på underrättelseförmågan och är i regel en längre och svårare process än för mera konventionella medel.

Den amerikanska organisationen, med dess processer och metoder, är väl utvecklad och prövad idag. Hur dessa ska användas finns tydligt och klart beskrivet i både gemensam och försvarsgrensvisa doktriner. Tillsammans skapar detta ett väl fungerande koncept.

---

[33] Maj Arthur Tulak *The Physical Destruction Component of Information Operations in Peace Enforcement* och *PSYOP C2W Information Operations in Bosnia* samt *Newsletter No.99-2 IO in a Peace Enforcement Environment*

IO-cellen som organisationsform skapar flexibilitet samtidigt som den kan användas på såväl strategisk som taktisk nivå. Genom att komplettera cellen med ”IO WG” säkerställer man synergieffekten av informationsoperations-insatser sett mot övriga tillgängliga medel. Vald organisationsstruktur underlättar även multinationella insatser där övriga deltagande nationer kan delta med de delförmågor dessa medför.

För att säkerställa samordningen mellan informationsoperationer och övriga medel i stabsprocesserna, exempelvis vid bekämpning, har man anpassat sig till dessas tidshorisonter. Man använder även samma typer av tabeller och matriser för planering och genomförande.

Vill man ha optimal uteffekt av sina informationsoperationer kräver detta kunniga chefer och välutbildade och samövade staber. Detta innebär att IO-cellen måste bildas så tidigt som möjligt och påbörja sin samövning. Vid insats bör det ske fortsatt utbildning och träning för att inte tappa förmågan till att använda alla medel och metoder. En del av tillgängliga medel kan vara förbjudna att användas enligt gällande lagar och bestämmelser vid, exempelvis, en PSO.

Baserat på dessa slutsatser och de erfarenheter som finns från genomförda stabsövningar på FHS bildar jag följande hypotes: *Den nuvarande amerikanska modellen för ledning och planering av informationsoperationer är direkt applicerbar för svenska förhållanden.*

3. Hur ser den svenska Försvarsmakten på informationsoperationer, som metod, över hela konfliktskalan?

3.1 Vad säger de officiella källorna

Jag kommer här att beskriva vad regeringen och försvarsmakten säger avseende organisation samt processer och metoder. Underlaget för detta stycke kommer främst från regeringens senaste försvarsproposition [34] samt regleringsbrevet [35] avseende försvarsmakten årsrapporter från perspektivplaneringen [36], utkast till militärstrategisk doktrin [37] samt grundsyn ledning.[38]

Regeringen behandlar informationsoperationer i många av delkapitlen i propositionen, men ägnar även området ett eget kapitel. I detta kapitel trycker regeringen på vikten av en nationell strategi för samhällets hantering av informationssäkerhet och skyddet mot informationsoperationer. Den nationella ledningen och samordningen bör ha en gemensam överblick, även tvärsektoriellt, och förmåga att med snabbhet kunna hantera dynamiken i dessa hot. En modell för detta är SUR-modellen (skydda – upptäcka - reagera) som beskrivs i propositionen 2001/02:10 Fortsatt förnyelse av totalförsvaret.

Problemen för den nationella ledning och samordning, enligt SUR-modellen, utgörs av att mycket av IT-tekniken och nätverken inte är statligt ägt och det utbredda beroendet av internationellt samarbete, såväl avseende ägande av och tillgången till information.

---

[34] Proposition 2001/02:10 *Fortsatt förnyelse av totalförsvaret*

[35] Regleringsbrev för budgetåret 2002 avseende Försvarsmakten

[36] *Försvarsmaktsidé och målbild Rapport 5, Årsrapport från perspektivplaneringen 2001-2002; Idébilder och fördjupningsområden inför Försvarsbeslut 2004 – rapport 6*

[37] Underhandsexemplar av *Remiss 1 – Militärstrategisk doktrin*

[38] *FM Grundsyn Ledning*

Regeringen avser att gå vidare med de förslag som Sårbarhets- och säkerhetsutredningen (SOU 2001:41) tagit fram för att möta hoten mot IT-säkerheten och från informationsoperationer. Detta skulle innebära att den nya planeringsmyndigheten ges det sammanhållande myndighetsansvaret för samhällets IT-säkerhet. För att understödja denna inrättas en funktion för teknikkompetens, en funktion för IT-incidenthantering samt ett system för evaluering och certifiering. Informationsunderlag till dessa funktioner och myndighet skapas genom regelbundna och övergripande omvärldsanalyser. Avseende hur, var och vem som ska inrätta dessa enheter kommer regeringen att återkomma till under våren 2002. Detta skedde den 14 mars med presenterandet av propositionen 2001/02:158 Samhällets säkerhet och beredskap. Innebörden i stort avseende informationsoperationer är: ett namnbyte från planeringsmyndigheten till Krisberedskapsmyndigheten samt en interimslösning avseende fördelningen av funktionerna som skall prövas under två år.

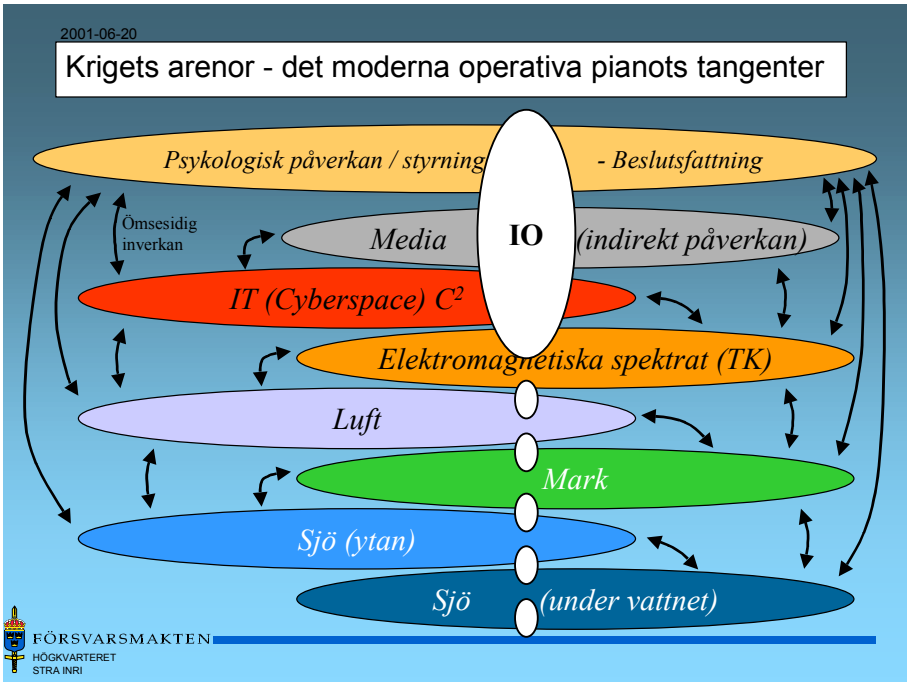
Konkreta åtgärder för att möta hotet från informationsoperationer vill regeringen nå inte bara nationellt utan även internationellt, främst i samarbete med övriga EU-länder. Detta kan exempelvis vara skapandet av en gemensam principiell grundsyn på skyddet. Regeringen poängterar att informationsoperationer har en betydande säkerhetspolitisk dimension. Innebörden är att informationsoperationer måste studeras, följas upp och analyseras ur både ett nationellt säkerhetsperspektiv och ett tvärsektionellt synsätt. [39]

Vid utformningen av det militära försvaret trycker regeringen på att förmågor och kompetens till informationsoperationer skall finnas där. När det kommer till det nätverksbaserade försvaret poängteras vikten av att generellt försöka undvika särskilda svenska lösningar. Vid försvar mot väpnat angrepp vill regeringen att försvarsmakten först redovisar förmågan att hantera

[39] Proposition 2001/02:10 *Fortsatt förnyelse av totalförsvaret*, Kapitel 10

informationsoperationer. Denna kompetens menar man skall innefatta kunskap om metoder för att planera och genomföra informationsoperationer, bland annat inom ramen för samordnade militära operationer. Utvecklingen av integrerade och flexibla stridskrafter och dess påverkan på utformningen av insatsorganisationen måste beakta att informationsoperationer kommer att ingå i de flesta olika typer av stridshandlingar. Slutligen trycker regeringen dels på vikten av goda kunskaper i hur informationsoperationer genomförs för att kunna verifiera egna vidtagna skyddsåtgärder, dels på att Försvarsmakten skall kunna lämna stöd till andra myndigheter. [40]

Vad säger då Försvarsmakten om informationsoperationer? Informationsoperationer pågår i fred, kris och krig och utgår från ett säkerhetspolitiskt perspektiv, samt inriktas mot stater eller andra säkerhetspolitiska aktörer. Det yttersta syftet är att påverka det mänskliga beslutsfattandet. Informationsoperationer kan struktureras i de olika arenor där man med information i någon form har möjligheten att påverka just denna beslutsprocess enligt bilden nedan.



[40] Ibid. kapitel 12 samt Regleringsbrevet från december 2001 s. 14 och 19

Inom varje arena finns såväl offensiva som defensiva förmågor.

Dagens informationssamhälle och det ömsesidiga beroende mellan Försvarsmakten och övriga delar av samhället ger informationsoperationer en karaktär av tvärsektoriell påverkan. Detta kräver en omfattande samverkan mellan olika aktörer. Det ömsesidiga beroendet kommer att fortsätta öka i takt med den fortsatta utvecklingen i världen. Effekten av påverkan visades tydligt i samband med händelserna i New York den 11 september 2001.

Den väpnade striden kommer även fortsättningsvis att spela en avgörande roll vid konflikthantering. Den som då har förmågan att nyttja informationsoperationer som en integrerad del av striden kommer att få en viktig effekthöjning av sina insatser. Exempelvis vid konflikter där svenska enheter deltar och vår etiska och moraliska uppfattning diametralt skiljer sig från motståndarens. Dessa skillnader kommer att skapa etiska dilemman med konsekvenser i form av vilka medel och metoder vi använder i striden där förmågan till informationsoperationer kan komma att vara avgörande.

Nätverksbaserad strid och själva kärnpunkten i ny krigföring – att alla resurser kan nyttjas optimalt i ett nätverk- skapar följande kriterier för framgång; Avgörande kommer att, oavsett konfliktnivå, vara förmågan att i alla dimensioner snabbt kunna genomföra en avvägd insats med möjlighet till rätt verkan i tid och rum. För att detta skall kunna nås krävs en helhetssyn avseende informationsoperationer, från den strategiska nivån ned till absolut lägsta.

Nyckelordet är samordning, Inom Försvarsmakten såväl som inom Totalförsvaret i sin helhet, vilken startar på den högsta politiska nivån och verkar nedåt via ordinarie ledningsnivåer. De idag enligt Försvarsmaktens grundsyn ledning gällande ledningsnivåerna för insatsledning är; Nationell strategisk (regering och riksdag), militärstrategisk (överbefälhavaren), operativ (normalt chefen för operativa insatsledningen, men kan i vissa fall vara chef för insatsstyrka) samt taktisk (normalt chef för taktiskt kommando, men kan i vissa

fall vara chef för insatsstyrka). [41] Försvarsmaktens vision och strävan är därför att fortsätta utveckla nätverkscentrerad krigföring, eftersom denna kraftigt förbättrar möjligheterna för denna samordning. Ur denna skapas möjligheten att, enligt manövertänkande, nå ett avgörande genom att slå motståndarens vilja och förmåga på det moderna stridsfältet.

[41] *FM Grundsyn ledning*, sid 16-18

3.2 Vilken uppfattning finns hos vissa nyckelpersoner?

De personer som jag genomfört intervju med är flottiljamiral Stefan Engdahl C STRA/INRI samt generalmajor Tony Stigsson C OPL. Frågeställningarna framgår av bilaga 3 och svaren och dokumentationen av dessa finns hos författaren. Jag inledde med den militärstrategiska nivån i intervju med Stefan Engdahl och avslutade med operativ nivå och intervju med Tony Stigsson.

På den militärstrategiska nivån gavs en bild av hur arbetet med införlivandet av informationsoperationer, inte bara i Försvarsmakten utan även övriga Totalförsvaret, pågår. Stefan Engdahl sitter bland annat med i en arbetsgrupp, AG skydd mot informationsoperationer, som är tillsatt av regeringskansliet. Kortfattat sker det nu ett flertal parallella arbeten av olika projektgrupper, inom olika myndigheter, som inte fullt ut är samordnade. Det som försvårar denna samordning är nuvarande ansvarsprincip och lagstiftning. Ansvarsprincipen innebär i korthet att den myndighet som har ansvaret för aktuellt område också ansvarar för samordningen av andra myndigheter. Här uppstår ett problem då informationsoperationer påverkar tvärsektoriellt. För att möta detta pågår en utredning tillsatt av regeringen hur den nya myndigheten, Krisberedskapsmyndigheten skall verka. [42] Engdahl uppfattar att det finns ett klart intresse och en ärlig ambition från den politiska nivån att utan onödiga dubbleringar finna en optimal lösning. Försvarsmakten har ännu inte tagit något beslut om hur informationsoperationer skall användas som metod. Orsaken till detta anges vara bristen på helhetssyn. STRA/INRI har huvudansvaret inom Försvarsmakten och har i avvaktan på uppstarten av en projektgrupp, tagit initiativet att inleda vad man kallar toppmöten avseende informationsoperationer. Vid dessa möten medverkar de övriga aktörerna i Totalförsvaret och ambitionen är att utveckla funktionen med stor transpararens, syftande till att undvika dubbleringar och avvikande

[42] Huvudprinciperna för vilka myndigheter som har vilket ansvar finns i regeringens proposition 2001/02:158 *Samhällets säkerhet och beredskap.* Ansvarig utredare av hur den nya myndigheten skall lösa sitt övergripande samordningsansvar är Ann-Louise Eksborg, vilken även förväntas bli den första generaldirektören för Krisberedskapsmyndigheten

uppfattningar om innebörden av informationsoperationer. Referens för utvecklingen av Försvarsmaktens förmåga är främst den amerikanska synen, men det pågår även konceptuella arbeten inom ramen för EU:s krishanteringsförmåga avseende informationsoperationer. De sistnämnda kan mycket snart komma att bli huvudreferens om dessa blir en verklighet. Ledstjärnan för svensk utveckling är att skapa organisationer och processer så lika våra samarbetspartners som möjligt. Informationsoperationer skall vara en naturlig och integrerad del av alla typer av militära operationer, inte minst i utvecklingen av det nätverksbaserade försvaret. Engdahl tar även upp det faktum att vi redan idag har kompetens och förmågor inom många av delfunktionerna, även om det ibland är enbart enstaka individer. För att gå vidare med metoden informationsoperationer ur ett helhetsperspektiv är projekt ”IO-förmåga” under initieringsfasen inom Försvarsmakten. Det övergripande syftet med projektet är: identifiera Försvarsmaktens nuvarande resurser och förmågor inom IO. Utarbeta underlag för försvarsbeslut 2004 för att Försvarsmakten skall kunna inrikta utvecklingen mot målbilden och därvid utarbeta en plan med delmål för kompetens och förmåga rörande doktrin, organisation, personal, utbildning, övningar samt materiel.

Vid intervjun med Tony Stigsson framkom en mycket klar och tydlig bild av hur informationsoperationer, och pågående utveckling, påverkar den operativa nivån idag. Den metod, avseende organisation och processer, som den Operativa Insatsledningen idag använder är i stort samma som hos CJTF-konceptet. Detta innebär i förlängningen en mycket snarlik lösning som förutom NATO även den amerikanska försvarsmakten använder. Ledningen av informationsoperationer planeras och leds av en mycket begränsad skara människor, precis som specialförband. Det viktiga är att komma ihåg skillnaden mellan passiva (defensiva) åtgärder och aktiva (offensiva) som alltid kräver regeringsbeslut. Främsta orsakerna till detta är känsligheten och oklarheterna avseende nationell samt internationell lag. Stigsson poängterar dock redan tidigt att han uppfattar bristen på helhetssyn såväl inom som utom Försvarsmakten, men att det finns en ärlig och ambitiös vilja från den politiska

nivån att utveckla den samlade förmågan till informationsoperationer. Stigsson anser att informationsoperationer används på strategisk och operativ nivå. Anledningen till detta är dels tidigare nämnd beslutsnivå för aktiva åtgärder, men även den kontraproduktiva effekt informationsoperationer kan få om dessa inte är samordnade med övriga militära insatser. Stigsson uttryckte även viss tveksamhet, främst under krislägen, avseende behovet av en svensk militärstrategisk nivå. Avseende anpassning till interoperabilitet mot våra samarbetspartners utgörs denna av anpassning i termer, procedurer och tidsperioder vilket medger enkel och snabb anpassning vid multinationella insatser.

3.3 Sammanfattning av den svenska synen

Sverige har, från den politiska ledningen, en klar och tydligt uttalad vilja om hur svensk förmåga till försvar mot informationsoperationer skall utformas. Det finns klara riktlinjer avseende hur detta skall ske;

- Hur hantera det internationella beroendet, vilket till viss del även löser problemet med att delar av exempelvis nätverk är i icke-statlig ägo.
- Undvika dubbleringar av funktioner m.m. inom svenska totalförsvaret.
- Vid utformandet av det nätverksbaserade försvaret inte skapa särskilda svenska lösningar utan säkerställa interoperabilitet med våra samarbetspartners.

Det som nu under pågående utrednings- och implementeringsarbete upplevs vara gränssättande är gällande ansvarsprincip och lagstiftning.

Vidare är inte viljan kring utvecklingen av vår offensiva förmåga lika tydlig. Här finns det vissa skillnader mellan uttalade ambitioner och praktiskt vidtagna åtgärder. Det var detta jag uppfattade till del som min kompletterande frågeställning: vad är egentligen den svenska Försvarsmaktens vilja avseende informationsoperationer? Skillnaden mellan ambitioner och åtgärder kan vara av varierande art:

- Frånvaron av politiskt tryck på frågan eftersom flera aspekter är oklara. En aspekt är den politiska känsligheten avseende insatser med offensiva

informationsoperationer, vilken i huvudsak grundar sig på tvetydigheterna i internationell lag och folkrätt. En andra aspekt är svårigheten med att identifiera vem det är som genomför angrepp mot en nation med informationsoperationer. En tredje är hur man skall se på informationsoperationsangrepp, är ett sådant att likställa med väpnat angrepp? Detta är enligt Kingdon processen med de existerande problemområdena.

- En annan förklaring kan vara att det inte finns en tillräckligt bred politisk samsyn inom området, vilket då skulle skapa en försiktighet i hur regeringen uttrycker sig. Enligt Kingdon processen gällande politiska realiteter.
- En helt annan förklaring skulle kunna vara att Försvarsmakten inledningsvis arbetat sakta utan märkbara resultat, men nu kommit till en punkt där man kan konkretisera sig och kan presentera en lösning för vissa offensiva förmågor. Enligt Kingdon processen med tillgängliga lösningar som inte är tillräckligt tydliga och allmänt kända.

Oavsett bakgrund eller förklaring till otydligheten finner jag att den i dagsläget inte har någon negativ påverkan av arbetet som pågår inom Försvarsmakten.

Den andra delen av svaret av min kompletterande fråga består av att Försvarsmakten ännu inte har besvarat frågan om hur den skall gå vidare med informationsoperationer. Arbetet med denna fråga pågår såväl inom Försvarsmakten som utom, exempelvis vid FHS, bristen eller faran är att dessa arbeten inte sker samordnat.

Två sätt att se informationsoperationer ur Försvarsmaktens perspektiv är: [43]

- IO på nationell (multinationell) strategisk nivå. FM deltar med resurser inom ramen för en IO som leds från regeringskansliet. [44] Övriga delar kan vara till exempel insatser avseende utrikes- och säkerhetspolitik, diplomati, nationellt samordnad informationstjänst och nationellt IT-säkerhetsarbete.
- IO av olika slag ingående som understöd till en militär operation vilken leds av FM mot fastställda militär strategiska/operativa/taktiska mål. Olika funktioner, främst FM egna resurser inom IO, samordnas som stöd till den militära operationen.

Sammanhanget med informationsoperationer för att få ut önskad effekt kräver en mycket klar och tydlig samordning, vilket inte rimmar med decentraliserad ledning. Risken för att få ett kontraproduktivt resultat beroende på disharmoni mellan de olika nivåerna, från nationell strategisk till taktisk, är för stor för att sådan ledning ska utövas. Effekten kan utgå från vilken nivå som helst över hela spektret, medan önskat resultatet av påverkan kan ligga på en helt annan nivå. Avslutningsvis kan sägas att det råder samsyn på såväl militärstrategisk som operativ nivå, för vikten av informationsoperationer som en naturlig och integrerad del av militära operationer, oberoende av vilken av huvuduppgifterna som löses.

3.4 Slutsatser

Det finns en tydlig och relativt gemensam syn på hur informationsoperationer skall användas i Sverige, såväl politiskt som militärt.

Det finns en skillnad mellan budskap och handling avseende offensiva informationsoperationer. Förklaringen till detta kan vara politisk, militär eller

---

[43] Enligt HKV STRA/INRI bildspel avseende *Försvarsmakten och Informationsoperationer*

[44] Författarens kommentar: På detta sätt borde även ledandet av IO-insatser ske vid användandet av svenska förmågor inom ramen för CJTF-konceptet (Combined Joint Task Force). Detta på grund av den politiska känsligheten i dessa typer av insatser och de effekter som kan uppstå.

en kombination av dessa. Oavsett vilken förklaring som finns begränsar inte detta i dagsläget utvecklingsarbetet av informationsoperationer som metod inom Försvarsmakten.

Gällande principer för myndighetsansvar och lagstiftning utgör en begränsning på nationell nivå, för hur man organisera sig och vilka processer som skall användas.

Försvarsmakten ser det yttersta syftet med informationsoperationer att påverka mänsklig beslutsfattning. Detta sker samordnat med övriga tillgängliga medel och kommer sannolikt alltid innehålla en komponent av fysisk bekämpning. Det är som konflikten i övrigt en kamp mellan olika viljor, vilket innebär att informationsoperationer alltid sker såväl defensivt som offensivt.

Försvarsmaktens nuvarande nivåindelning underlättar väsentligt interoperabiliteten vid multinationella operationer, men kan utgöra en begränsning för nationella operationer i krislägen. Sveriges geografiska storlek och tillgängliga stridskrafter innebär att det är tveksamt om det kommer avdelas mer än ett operationsområde. Om så är fallet finns det då ett behov av en militärstrategisk nivå mellan den operativa och national strategiska? Gynnar eller missgynnar detta ledning och planering?

Nuvarande organisation, processer samt tidshorisonter på den operativa insatsledningen och taktiska staber är direkt kompatibelt med våra samarbetspartners, vilket medger lika arbetsmetoder vid såväl nationell som multinationell operation.

Det finns ett stort kunskaps- och kompetensbehov inom Försvarsmakten och övriga Totalförsvaret för att kunna driva utvecklingen vidare, men inte minst att kunna påverka den mentala inställningen till informationsoperationer. I dagens diskussioner är det en överdriven fokusering på nätverkskrigföring och helheten går till del förlorad.

4. Finns det några avgörande skillnader mellan svensk och amerikansk syn på informationsoperationer?

4.1 Definitioner och omfattning av informationsoperationer

Jag kommer här att fokusera på följande begrepp; informationsoperationer, informationskrigföring, offensiva informationsoperationer samt defensiva informationsoperationer. [45]

Informationsoperationer (IO) - Riktade och samordnade åtgärder till stöd för egna politiska och/eller militära mål genom att påverka eller utnyttja motståndarens eller annan utländsk aktörs information och/eller informationssystem. Det yttersta målet är att påverka det mänskliga beslutsfattandet. IO kan genomföras i såväl politiska, ekonomiska som militära sammanhang.

Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO.

Vid en första anblick framgår det två tydliga skillnader mellan de båda definitionerna, nämligen att den svenska trycker på det yttersta målet – *"att påverka det mänskliga beslutsfattandet"*. I den amerikanska trycks det på både "*affect adversary…while defending one´s own"*. Vilka innebörder får dessa skillnader?

Sett mot den första, avseende det yttersta målet att påverka det mänskliga beslutsfattandet, blir inte skillnaden avgörande. Detta då amerikanarna, i samband med definitionen, sätter denna i förhållande till helheten. Vilket man anger är att påverka den informationsbaserade beslutsprocessen för att nå det avgörande målet – att påverka motståndarens beslutsfattare.[46] Orsaken till

---

[45] Svenska definitioner enligt underbilaga 1 till skrivelsen 23 210:62 285, *Årsrapport från perspektivplaneringen 2001-2002; Idébilder och fördjupningsområden inför Försvarsbeslut 2004 – rapport 6,* s. 162. Amerikanska definitioner enligt *Joint Pub 3-13* samt *MCWP 3-36*

[46] *Joint Pub 3-13* s. vii-viii

skillnaderna i definitionerna upplever jag vara att amerikanarna lyfter fram sin definition i det stora sammanhanget där man direkt knyter syftet med offensiva och defensiva förmågor. Amerikanarna kopplar även tidigt in vikten av att redan före eller precis i uppstarten av en kris sätta in informationsoperationer för att nå optimal effekt.

Nästa skillnad i definitionerna blir mer intressant. Den svenska definitionen tar inte upp försvaret mot informationsoperationer utan talar enbart om påverkan av någon form av motståndare. Med detta menar jag att från regeringens sida främst talar man om förmågor för försvar mot informationsoperationer, inte vilka offensiva sådana vi själva skall ha. Förklaringen till detta kan vara dels den politiska känsligheten och den oklara lagstiftningen, dels försöka att verka avskräckande mot eventuella motståndare. I proposition 2001/02:10 Fortsatt förnyelse av totalförsvaret på sidan 101 i fotnotstexten, förs ett resonemang kring definitionen av IO. Där nämns metoden att skydda egen information och informationssystem. I diskussionen påtalas även att denna formulering finns i definitionen av IO i Sårbarhets- och säkerhetsutredningen (SOU 2001:41). Denna formulering avseende skyddet av egen information och informationssystem i definitionen av IO finns dock i årsrapporten från perspektivplaneringen 99-00. [47] Varför denna ordalydelse sedan har kommit att ändras i Försvarsmaktens kommande rapporter och arbeten vet jag inte svaret på. Det kan vara så enkelt att det är ett redigeringsmisstag som fortlever, jag har inte funnit något som visar på att det skulle vara ett medvetet beslut. Oavsett vilken förklaring som finns skapar det, enligt min uppfattning, en viss tvetydighet i den svenska viljan avseende informationsoperationer när man enbart studerar officiella dokument. Jag har under mitt arbete, såväl praktiskt vid övningar som vid intervjuer, däremot inte funnit något som styrker att detta negativt skulle påverka den utveckling och forskning som bedrivs i Sverige.

---

[47] *Försvarsmaktsidé och målbild Rapport 4*, s.158

Informationskrigföring - Informationsoperation som genomförs under kris och krig för att främja eller uppnå särskilda politiska och/eller militära mål gentemot en eller flera motståndare.

information warfare. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called IW.

Synen på begreppet informationskrigföring skiljer sig inte mellan svensk och amerikansk definition. Den skillnad jag uppfattat, under arbetets gång, är synen på att ta till offensiva åtgärder, med andra ord gå från informationsoperation till informationskrigföring. Jag finner inte detta märkbart med anledning av de båda nationernas säkerhetspolitiska ambitioner och historia. Diskussion om SUR-modellen (skydda – upptäcka - reagera) förekommer i båda nationerna. Hur snabbt kan man i praktiken uppfatta och eventuellt agera mot informationsoperationer, vilka kriterier skall finnas för att gå från defensiv till offensiv samt vad säger nationell och internationell lag? Denna diskussion är mycket intressant och påverkar, enligt min bedömning, både organisation, processer som metoder. Vad säger då respektive nation om definitionen av förmågor att tillämpa informationsoperationer?

Offensiva informationsoperationer (IO-O) - Riktade och vanligen samordnade åtgärder i fred, kris och krig för att påverka en motståndares information och/eller informations- och kommunikationssystem. Målet är bland annat att påverka dennes förmåga till rationellt beslutsfattande och därmed gynna egna syften. Genomförs t.ex. genom fysisk attack/förstöring, vilseledning, skydd mot informationsinhämtning, telekrig och psykologiska operationer.

offensive information operations. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisionmakers to achieve or promote specific objectives. These capabilities and activities include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations, and could include computer network attack

Inte heller i definitionen av offensiva informationsoperationer föreligger några direkta skillnader, men hur ser det ut i tillämpning och verklighet? Har Sverige någon möjlighet att leva upp till förmågorna? Både teknik och kunskap för att nyttja ”computer network attacks” finns inom Sverige. Vi är och har länge varit en av de ledande nationerna inom IT-kommunikation och växelsystem. Det som blir begränsande är återigen den politiska känsligheten samt nationell och internationell lagstiftning, vilket innebär att även om förmågan finns kommer det alltid att krävas ett politiskt beslut för att nyttja denna. Fördelen med denna förmåga, sett mot Försvarsmaktens huvuduppgifter, är att understöd av exempelvis utlandsstyrkan i en militär operation kan ske från Sverige via det globala nätverket. Omvänt sker också defensiva åtgärder som ”computer network defence” på ett motsvarande sätt. Idag sitter exempelvis IT-säkerhetschefen för Kosovobataljonen på SWEDINT i Almnäs. Telekrig är något som vi svenskar länge har varit duktiga på avseende skyddsåtgärder, nytt är att vi sedan några år även bygger upp en mer offensiv förmåga. Psykologiska operationer är i Sverige en ny förmåga, konkret består den av ett antal individer med kompetens från olika utbildningar, bland annat i USA.

Detta gör att vi i realiteten inte idag har en operativ sådan förmåga. Kunskapen på militärstrategisk och operativ nivå om svårigheterna och komplexiteten med psykologiska operationer finns och framkom under mina intervjuer.

Defensiva informationsoperationer (IO-D) - Riktade och vanligen samordnade åtgärder i fred, kris och krig avseende operationer, personal, teknologi och policy för att skydda och försvara information, informationssystem och egen förmåga till rationellt beslutsfattande. Genomförs t.ex. genom fysiskt skydd, skydd mot vilseledning, skydd mot informationsinhämtning, säkerhetsunderrättelsetjänst och telekrigsåtgärder och psykologiskt försvar.

defensive information operations. The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes

Även avseende defensiva informationsoperationer tyder det på en samsyn mellan svensk och amerikansk definition. Tillämpningen av dessa, enligt vad jag kommit fram till, skiljer sig inte heller markant. Förklaringen till detta finns dels i det moderna informationssamhället, dels i den ledande ställning USA har inom informationsoperationer och den påverkan detta medför. I både USA och Sverige har det skett utredningar, med kraftsamling till skyddet av olika nätverk, för att skapa ett nationellt tvärsektoriellt skydd. De förslag till lösningar som finns är mycket snarlika. Se under punkten 3.1 tidigare i uppsatsen.

Sammanfattningsvis, avseende definitioner och omfattning av informationsoperationer i Sverige, påstår jag följande; förmågorna finns till delar sedan tidigare. Det nya är sättet hur vi skall samordna dessa, det vill säga hur vi ska organisera oss samt vilka processer och förmågor vi vill kunna nyttja.

4.2 Ledning och planering

Inledningsvis hur ser svensk indelning avseende nivåer ut och hur har vi valt att organisera oss jämfört med amerikanarna? Sedan FM Grundsyn Ledning kom år 2001 och den genomförda omorganiseringen av den militära ledningen, har vi kommit att ha samma nivåindelning.

I Sverige utgörs den strategiska nivån av den nationella (regering och riksdag) samt militärstrategiska (ÖB med stabsfunktion i STRA/INRI). Jämför man vad dessa skall lösa för uppgifter och vilket ansvar de har avseende planering och ledning, hittar vi på pappret inga direkta skillnader. Den stora skillnaden utgörs främst av det statsskick som finns i respektive land innebärande en, i alla konfliktnivåer, klarare, starkare och kanske snabbare politisk styrning i USA. USA har vad som normalt kallas ministerstyre vilket innebär att ministern är den som fattar beslut och är ansvarig. I Sverige lyder ämbetsverken (Försvarsmakten) direkt under regeringen men sorterar under departementen. Departementschefen, ministern, får inte direkt blanda sig i ämbetsverkets beslutsprocess, utan denne är i huvudsak sysselsatt med planering och utformning av regeringspolitiken. Dock ur ett strikt svenskt nationellt tänkande utgör inte detta någon avgörande begränsning för insatsledning. Det pågår nu en ny ledningsutredning inom svenska Försvarsmakten som bland annat ser över ansvar- och rollfördelningen mellan våra nivåer. Under pågående arbetet finns det en diskussion inom Försvarsmakten där vissa ifrågasätter behovet av en militärstrategisk nivå, likväl som andra förordar en samlokalisering av Försvarsdepartement och Högkvarter (utan att för den delen övergå till ministerstyre). Sett ur ett informationsoperationsperspektiv skulle en utveckling liknande den sista underlätta planering och ledning ur ett nationellt perspektiv.

På operativ nivå har vi en Operativ insatsledning, indelad enligt samma sektionsindelningsprincip som USA. En sektion är ett antal människor som arbetar med och företräder en specifik funktion, exempelvis, underrättelser. En stab består sedan av ett antal sektioner som leds av en stabschef. På grund av sin storlek och globala engagemang har USA ett flertal ”regional commands” för operativ planering och ledning. Det viktiga är inte antalet utan det faktum att avseende planering och ledning har man ett likartat ansvar i de båda länderna. För att underlätta planering och ledning har vi i Sverige valt att samlokalisera de taktiska kommandona med den Operativa insatsledningen.

Det för oss in på den taktiska nivån där våra olika staber också är indelade enligt samma struktur som USA. I den planering och ledning som genomförs utgör de taktiska kommandona, samt 1. Mekdivisionstaben, motsvarande nivå som en ”component commander”. Dessa är normalt taktiska chefer, men kan i vissa fall komma att verka som ”commander joint task force” beroende på uppgift.

Vilken ledningsmodell används då av organisationen? Svenska försvarsmaktens agerande skall präglas av ett manövertänkande där ledningsmetoden är uppdragstaktik. Planering i förhandsläge sker ofta centraliserat medan genomförandet är decentraliserat. Motsvarande syn har amerikanarna i dag, vilket för deras del sett ur hela det amerikanska försvaret är relativt nytt. Amerikanarna har tidigare, främst inom US Army, haft en klart centraliserad ledning och mer kommandostyrning än uppdragstaktik. När vi ser till ledning och planering av informationsoperationer finns det ett behov av en centraliserad ledning av funktionen. Ser vi till de erfarenheter som amerikanarna dragit under de sista tio åren finns det en naturlig förklaring till detta. Eftersom effekten och resultat av denna typ av operationer mycket snabbare än något annat medel kan trycka ihop nivåerna. Detta innebär dock inte att planering och ledning inte sker på samtliga nivåer. Den styrande målsättningen att påverka motståndarens beslutsfattning kräver på det moderna

slagfältet, oavsett konfliktnivå, en stenhård samordning och koordinering för inte riskera att bli kontraproduktivt.

Vilka processer och metoder används då för att genomföra planering och ledning? I Sverige är beslutet tagit att på operativ nivå använda och tillämpa GOP (Guidelines For Operational Planning) i tillämpliga delar, vilket gör att det på denna nivå finns en mycket snarlik modell. Skillnaderna mot USA utgörs idag främst av kulturella skillnader som exempelvis chefens roll, byråkrati samt gradfixering. Båda försvarsmakterna talar om planering med gott om tid till förfogande samt planering under tidspress. Praktiska konsekvenser av vald modell och vårt allt större internationella agerande gör att vi har anpassat oss till de tidshorisonter, 24h, 48h och 72h, som också används i USA. Dessa tidsaspekter är knutna till de olika processer som finns inom organisationen, exempelvis ”targeting-processen”. Denna anpassning är gjord ända ned till taktisk nivå, vilket tydligt framkom under genomförd ASSÖ (Arméns Stabs och Sambands Övning) 02 i Enköping.
Med anledning av att vi använder samma processer i planering och ledning har vi även börjat använda samma metoder. För att återigen knyta an till ”targeting” genomförs det nu ”JCTB” och tillhörande arbetsgrupper på de olika nivåerna. Samma termer, tabeller och matriser för att metoderna skall fungera, används också. Vi använder också samma orderstruktur som USA med en ”main body” och ”annex”, främst på operativ och taktisk nivå. Det som Sverige saknar idag är, i de flesta fall, förmågorna för effekt, i form av vapensystem. Valet är medvetet av regering och ÖB sett mot aktuell hotbild och förändringen som pågår av Försvarsmakten. Motivet kan på ett tydligt sätt belysas med följande citat; ”Personalens kompetens är den viktigaste faktorn för god anpassningsförmåga i ledningssystemet, både på kort och lång sikt”. [48]

Efter denna jämförelse av organisation, processer samt metoder är det dags för en sista kontroll avseende synen på planering. Amerikanarna har i sina

[48] *FM Grundsyn ledning*, s. 27

doktriner listat ett antal framgångskriterier för planering av informationsoperationer. [49] Efter inläsning, deltagande i övningar samt genomförda intervjuer finner jag i de flesta fall inga avvikelser. Det som kan diskuteras är om förståelsen för vikten av strategisk underrättelsetjänst samt svårigheten med verkansbedömning av gjorda insatser finns. Strategisk underrättelsetjänst skapar ett underlag för insats av informationsoperationer och utgör en av nycklarna till framgång. För svenska nationella operationer uppfattar jag ändå att förmågan till stor del finns inom MUST. Här är det mer frågan om viss ominriktning och andra spaningsfrågor. Vid en multinationell operation, inom ramen för PARP eller EU krishanteringsförmåga, kommer denna förmåga att finnas.

4.3 Slutsatser

Avseende den övergripande synen på informationsoperationer finns det inga avgörande skillnader mellan svensk och amerikansk syn. Skillnaderna som finns är mer av semantisk och praktisk art .

Den stora, och inte minst naturliga, skillnaden är förmågan att genomföra informationsoperationer. I Sverige bör det finnas mer förmågor än vad som framgår av pappret: Exempelvis borde det genom att kombinera personer med PSYOPS-utbildning med de resurser som finns hos HKV/Info, gå att skapa en operativ förmåga för psykologisk krigföring.

Den mest begränsande faktorn för en nationell samordning av informationsoperationer i Sverige bedöms utgöras av myndighetsansvarsprincipen och gällande lagstiftning.

Den mest styrande faktorn för att nå framgång med informationsoperationer är valet av organisation. Ur denna kommer sedan processer och metoder för planering och ledning, vilket sedan säkerställer att den samordning som är nödvändig sker på ett effektivt och rationellt sätt.

---

[49] Denna uppsats s. 21-22.

Svensk anpassning avseende insatsledning till internationell standard gör att det med relativt enkla medel går att redan idag införa en modell för planering och ledning av informationsoperationer inom Försvarsmakten. En sådan skulle kunna användas vid såväl nationella som internationella operationer.

5. Prövning av hypotes

Efter att nu ha sammanställt den amerikanska doktrinen för informationsoperationer, undersökt den svenska viljan och ambitioner avseende dessa operationer och sedan jämfört dessa i sökandet av avgörande skillnader eller begränsningar kommer jag nu att slutligen pröva min hypotes. *Den nuvarande amerikanska modellen för ledning och planering av informationsoperationer är direkt applicerbar för svenska förhållanden.* Prövningen baserar sig på de slutsatser jag dragit och redovisat i uppsatsen mot komponenterna; *organisation, processer* och *metoder*. Jag kommer att avsluta med ett kritiskt granskande av mitt arbete.

IO-cellen som *organisation*?

Fördelen med IO-cellen är att den kan användas på samtliga nivåer och skapar en flexibilitet för att kunna växa och minska beroende på tillgängliga förmågor för informationsoperationer. Vidare är det en internationellt beprövad och använd organisation, vilket medger en likartad organisation vid såväl nationella som multinationella operationer. Flexibiliteten, främst på strategisk och operativ nivå, medger att denna organisationsmodell kan användas vid lösandet av Försvarsmaktens huvuduppgifter. Sett till de begränsningar dagens myndighetsansvar och lagstiftning ger i Sverige skapar denna organisation också en möjlighet till nationell tvärsektoriell samordning på den strategiska nivån. Genom att man organisera sig på detta sätt, över nivåerna, skapas troligtvis också bästa möjliga förutsättningar för vald svensk ledningsmetod, uppdragstaktik.

De *processer* som ingår i helheten i form av informationsoperationer är bland annat målval (”targeting”) och information. Vald planeringsmodell, främst på

operativ nivå, är också att se som en process. De åtgärder som redan är vidtagna i Sverige i form av indelning av staber, nyttjandet av GOP och tidshorisonter säkerställer att grundstommen kan tas ur motsvarande amerikanska. De skillnader som finns i tillämpning av dessa processer, främst kulturella, begränsar inte. Denna anpassning blir en styrka vid multinationella operationer, då vi med tempo och lätthet snabbt kan komma in i det praktiska arbetet. Genom att använda processerna skapas också ett underlag för vilka förmågor vi har eller vill utveckla för nationella operationer.

De *metoder* som gör att organisation och processer fungerar. Införandet av en ”IO Work Group” är väsentligt för att säkerställa koordineringen med andra insatta medel. Denna arbetsgrupp bör träffas innan ”JCTB” på operativ och taktisk nivå. Oavsett nivå skall den träffas före eventuella dagliga pressgenomgångar för att säkerställa ett ensat budskap. Eftersom det yttersta målet är att påverka mänskligt beslutsfattande, där en perceptionsstyrning är en stor arena, måste det budskap som går ut vara samordnat. Det enkla faktum att vi börjat använda samma orderstruktur som amerikanarna underlättar också ett bruk av deras övriga metoder, matriser m.m. Denna relativt enkla, men ändå viktiga faktor, bäddar också för en centraliserad samordning vilket medger viss form av uppdragstaktik även för informationsoperationer. Syftet med de metoder vi talat om är säkerställa att informationsoperationer blir en naturlig och integrerad del i den operativa verksamheten.

Vilka brister finns det i det underlag som jag baserar denna analys och värdering på? Den kanske största är avsaknaden av intervjuer med amerikansk personal som har arbetat med informationsoperationer (all information är från officiella verk). Denna brist har jag försökt möta genom diskussioner med Anders Johansson vid ISS på FHS, som har praktisk erfarenhet av samarbete med amerikaner i Bosnien. Under de övningar på FHS där jag gått i befattning, har vi även använt amerikansk organisation, processer och metoder så långt som möjligt. Vad avser den svenska synen och viljan för informationsoperationer har jag enbart intervjuat nyckelpersoner inom

Försvarsmakten. Dessa har i sig gett en bild av läget på nationell nivå utanför Försvarsmakten. Jag har tagit del av de rapporter och propositioner som finns, tillsammans bekräftar de bilden av en minst sagt dynamisk fas i utvecklingen av svensk syn och vilja. Med anledning av min problemformulering och ambitionen att skapa en ledningsmodell bedömer jag inte avsaknaden av dessa amerikanska intervjuer vara avgörande.

6. Hur skulle en svensk ledning och planering av informationsoperationer kunna ske vid försvar mot väpnat angrepp?

6.1 Inledning och beskrivning av scenario

För att skapa spårbarhet i detta sista kapitel har jag valt att utgå från en av de idébilder som används under perspektivplaneringen inom Försvarsmakten. [50]

Förutsättningen i denna idébild är:
Sverige stödjer vissa staters territoriella integritet främst genom framgrupperade underrättelse- och övervakningssystem. Gotland har en avgörande betydelse för Försvarsmakten, främst avseende basering av sensorer och långräckviddiga bekämpningssystem. Ledningen av Försvarsmakten sker enligt dagens principer. Den civil-militära samverkan har vidareutvecklats och gått mot en mer långtgående tvärsektoriell samverkan. De flesta av de förslag som kom med Sårbarhetsutredningen har genomförts vilket höjt samhällets skyddsnivå mot främst terrorism och liknande. Skyddet mot informationsoperationer har påbörjats men vissa utredningar om lagar och förordningar pågår fortfarande. De svenska stridskrafterna har god förmåga till ledning och planering av insatser med allsidigt sammansatta stridsgrupper (joint task forces) även på den taktiska nivån. Initialeffekten har samlats mot försvaret mot fjärrstridskrafter och bekämpning av de samma, den stora begränsningen är avsaknaden av skyddssystem mot ballistiska missiler.

[50] Idébild A – ”Väpnat angrepp”, *Försvarsmaktsidé och målbild Rapport 5*, s. 135

6.2 Exemplifiering

Strategisk nivå

Huvudinriktningen på denna nivå är att fastställa de övergripande nationella målsättningarna och önskat slutläge (”end state”) samt ge uppgifter och resurser till Opil. Under pågående operationer fyller den i första hand en övervakande roll och styr med prioriteringar, det finns dock ett stort undantag - nätverkskrigföring. Nätverkskrigföring (både defensiv och offensiv) planeras, genomförs och utvärderas av den strategiska nivån. Motivet till detta är främst; behovet av tvärsektoriell samordning, beroendet av internationella nätverk, komplexiteten i nationell samt internationell lagstiftning samt inte minst svårigheten att bedöma effekter vid insatser samt risken för oönskade sidoeffekter (”Collateral damage”). Sammantaget gör dessa faktorer att det alltid kommer att krävas en mycket starkt centraliserad och politiskt styrd ledning av dessa insatser. Den tekniska utvecklingen gör också att det inte är gränssättande vare sig på vilken nivå eller plats du fysiskt sitter för denna typ av informationsoperationer.

Indelning av den nationella strategiska IO-cell som finns vid den gemensamma ledningsplatsen: Sammankallar och leder gör representant från Regeringskansliet

Repr RK (leder arbetet)		
STRA/INRI	MUST	HKV/INFO
Specialförband	FRA	PSYOPS
FoI (CNA/CND)	SÄPO	Polisens IT-incidentC
Krisberedskapsmyndigheten	PTS	”Nätverksägarförening”
Legal (Jurist)	Politisk rådgivare (ev)	

Ur dessa enheter bör representanten vara den i fred ordinarie handläggaren av informationsoperationer. Vidare tillkommer vid behov eventuella andra samverkanspersoner från understödjande enheter och funktioner.

Denna IO-cell är under planering ansvarig för framtagande av;

- Nationella målsättningar för informationsoperationer och önskade ”end state”.
- Tar fram strategiska ”centre of gravity” såväl motståndarens som egna.
- Fastställer eventuella begränsningar eller styrningar för operativ chef.
- Tilldelar uppgifter och resurser till operativ chef.

Uppgifter som löper över planering och in i genomförande;

- Sammanställer en gemensam nationell omvärldsbild avseende IO.
- Beslutar om insats av eventuella strategiska reserver.
- Leder och samordnar försvar mot nätverksattacker.
- Inhämtar underlag för egna nätverksattacker mot motståndaren.
- Understödjer övriga nivåer med nätverksattacker och bekämpning efter ”eldtillstånd” av regering/krigsdelegation.
- Ger tillstånd för fysisk bekämpning av tidigare strategiskt utpekade ”restricted targets” efter hemställan från operativ chef.
- Inhämtar underlag för utarbetande av teman/mål för psykologiska operationer.
- Fastställer och beordrar teman/mål för psykologisk krigföring.
- Svarar för framtagande av IO-ROE, handlägger ROE-begäran under pågående verksamhet.

För att kunna svara upp mot de uppgifter som är av mer löpande karaktär finns det en VB-funktion IO som utgörs av följande personer ur IO-cellen;

- Representant STRA/INRI (normalt ansvarig IO-hl)
- Representant från HKV/Info
- Representant Psykologiska operationer
- FoI (FMV) som svarar för CND/CNA
- Representant för Krisberedskapsmyndigheten (IO-hl)
- Legal

Operativ nivå, den Operativa insatsledningen

Denna nivå är navet för planering och genomförande av svenska informationsoperationer och i följande huvudprocesser måste funktionen vara representerad för att säkerställa koordinering och effekt;

- Planering i ”Joint Operational Planning Group – JOPG”.
- Bekämpning i ”Joint Coordination Targeting Board – JCTB” med tillhörande förarbetsgrupp ”JTWG”.
- Genomförande i ”Joint Operations Centre – JOC”.

För att möta dessa behov finns en kärna av IO-officerare tillhörande J3. Deras huvuduppgifter är;

- Sammankallar och leder IO-cellen.
- Leder AG IO och deltar i ”JTWG” samt ”JCTB”.
- Bemannar ”JOC” och övervakar genomförande.
- Beredd ingå i ”JOPG” under J5.

Denna kärna förstärks sedan med en IO-cell samt en Arbetsgrupp IO.

För planering av informationsoperationer finns IO-cellen;

Repr J3 (leder arbetet)		
Representant J2	Representant J4	Representant J5
Representant J6	Representant Telekrig	Representant PSYOPS
Representant PIO	Representant MTK	Representant FTK
Representant MekDiv	Representant Specialförb	Legal (Jurist)
Politisk rådgivare (ev)		

Utöver dessa kan det tillkomma samverkanspersonal från andra understödjande enheter, exempelvis IT-säkerhetsförband.

Uppgifter under planering;

- Analyserar strategiskt ”Initiating Directive”.
- Tar fram operativ ”centre of gravity” såväl motståndarens som egen.
- Analyserar och identifierar motståndarens kritiska sårbarheter m.m.

- Utarbetar en IO-plan, med såväl offensiva som defensiva åtgärder, som understödjer den operativa idén.
- Utarbetar följande arbetsunderlag för genomförande; ”IO Goals and Objectives”, ”IO Synchronization Matrix” samt ”IO Target List”.
- Utarbetar behov av underrättelser för att stödja IO.
- Utarbetar resursbehov och jämför med tilldelning.
- Utarbetar förslag på prioriteringar avseende bekämpning.
- Utarbetar aktuella Annex i Operationsordern.

För den fortlöpande verksamheten (”JOC” och ”JCTB”) finns AG IO. Bestående av representanter ur följande sektioner; J3 (leder), J2, J4, J5, J6, PIO samt representanter för Telekrig och PSYOPS. Arbetsgruppen träffas dagligen innan ”JCTB” och följer denna agenda;

1. Närvarokontroll
2. Aktuellt läge (J2/J3)
3. Fi läge och stridsvärde (24-72 h, J2)
4. Kommande egen planering (J3)
5. Bedömning och översyn av IO-verksamheten med tonvikt på bekämpning.
    a. Senaste 24h
    b. Kommande 24h (fastställa mål, nya undbehov m.m.)
    c. Kommande 48h
    d. Kommande 72h
6. Övriga händelser (exempelvis kommande pressbriefings)
7. Eventuella arbeten med Frago[51] eller liknande
8. Avslut

[51]Författarens kommentar: Frago (Fragmentary Order) är en förenklad order som reglerar och styr en viss bestämd aktivitet inom ramen för en Operationsorder.

Taktisk nivå

I detta fall redovisas indelningen vid 1.Mekaniserade Divisionen. På taktisk nivå är det mer frågan om ett verkställande, främst telekrig och fysisk bekämpning, av på operativnivå planerade insatser och kampanjer. Behovet av ett antal personer med IO-kompetens finns även här för att kunna leda IO-cellen, delta i planerings- och ledningslaget samt bemanna VB i StriC.

Grundelementet är IO-cellen vars främsta funktion är att säkerställa att planerade informationsoperationer inte påverkar egen taktisk stridsplan.

Repr S3 (leder arbetet)		
Representant S2	Representant S4	Representant S5
Representant S6	Representant SISBat	Representant Undbat
Representant Bek	Representant Jbat	Representant PIO

Cellen samlas normalt en gång per dygn innan ”JCTB”.

Uppgifter;

- Rapporterar mållägen till högre chef.
- Rapporterar verkansbedömningar till högre chef.
- Omvandlar beordrad IO-verksamhet till bekämpningsordrar för ingående förband och förmågor.
- Identifierar och rapporterar uppåt egna underrättelsebehov.

6.3 Slutsatser

Efter denna exemplifiering, vilka konsekvenser skulle detta innebära för Försvarsmakten och hur kan man se på dessa?

Samlokaliseringen av huvudaktörerna, eller vissa ingående funktioner, på den strategiska nivån redan i fredstid skulle underlätta omställningen och förkorta reaktionstider inom ramen för informationsoperationer.

För att kunna utöva vissa av de offensiva förmågorna, exempelvis, psykologiska operationer kommer det att ställas nya krav på vår strategiska underrättelsetjänst.

Det krävs förutom en allmän översyn av lagsystemet framtagande av ROE för informationsoperationer för hela konfliktskalan.

För att erhålla en trovärdig och effektiv svensk nationell förmåga till informationsoperationer krävs utveckling och införskaffande av vissa förmågor.

Många av de exklusiva resurserna kräver en välutbildad personal för att vara effektiva. Detta borde gå att lösa med kontraktsanställning och en översyn samt viss kompetensutveckling av redan idag tillgängliga reservofficerare.

För att säkerställa en snabb och funktionell övergång till ledningsmodellen i kris krävs att denna är känd och övad i fred. Ett sätt att göra detta är att viss personal tjänstgör och placeras i befattning redan under fredstid, exempelvis, på STRA/INRI, respektive sektion 3 och 5 på Opil, de taktiska kommandona samt divisionstaben.

För att säkerställa både tempo och kontinuitet i införandet av och förändring av inställningen till informationsoperationer i Försvarsmakten borde det bildas ett center motsvarande SkyddC för funktionen. Detta center och i förra slutsatsen nämnda befattningar skapar även en möjlighet till kontinuitet och fortsatt utveckling av informationsoperationer i Försvarsmakten.

6.4 Förslag till framtida studier

Under mina studier av informationsoperationer och framtagandet av en ledningsmodell har jag funnit andra spår som skulle ha varit intressanta att undersöka.

En studie skulle kunna omfatta hur skall den tvärsektoriella nationella svenska samordningen ske av informationsoperationer? Är det så att med de förslag som finns och bildandet av Krisberedskapsmyndigheten vi har en möjlighet till

en relativt snabb process? Vilka konsekvenser får en svensk nationell samordning på det internationella planet? På vilket sätt avser vi nyttja Försvarsmaktens förmågor i denna lösning?

En annan studie skulle kunna inrikta sig på området kompetenssäkring av informationsoperationer inom Försvarsmakten. Är det dags för ett fjärde taktiskt kommando eller är det ett nytt funktionscentra som behövs? Vilket säkerställer bäst såväl kompetens som att informationsoperationer blir en integrerad del av den operativa verksamheten?

En tredje studie skulle kunna inriktas mot förmågor och lagar. Vilka förmågor har vi idag i Sverige som nation och vilka avser vi utveckla? Vilka ROE skall gälla för dessa sett mot både nationell och internationell lag?

7. Sammanfattning

7.1 Syfte

Syftet med uppsatsen är att ta fram en svensk modell för planering och ledning av informationsoperationer. Denna modell skall kunna användas vid såväl nationella som multinationella operationer, men även oberoende vilken av Försvarsmaktens huvuduppgifter det gäller.

7.2 Material

Det material jag har undersökt består av artiklar och böcker som behandlar informationsoperationer, annan litteratur som berör ledning och planering av militära operationer, rapporter från olika arbetsgrupper, intervjusvar, propositioner och erfarenheter från övningar och genomförda operationer.

7.3 Metoddiskussion

Utgångspunkten i min metod har varit min problemformulering, hur skulle svensk ledning och planering av informationsoperationer kunna ske? Detta har gjort att jag använt en utvecklad kvalitativ metod. Först en undersökning av tillgängligt material vilket ledde fram till en hypotes och vissa slutsatser. Därefter genomförde jag intervjuer med vissa nyckelpersoner. Avslutningsvis jämförde jag mina resultat och det som framkom i intervjusvaren och skapade en modell som även exemplifieras.

7.4 Teorianknytning

Som analysverktyg för undersökning och jämförelse har jag använt van Crevelds teori och modell från boken ”Command in War”. Teorin grundar sig på att ledning i sig är en process som använder information för att koordinera människor och ting att utföra ett uppdrag med en gemensam målsättning. Denna process går att studera och analysera om den bryts ned i tre huvudkomponenter; organisation, procedurer och metoder samt tekniska hjälpmedel.

7.5 Hur ser den amerikanska doktrinen för informationsoperationer ut?

Den amerikanska organisationen, med dess processer och metoder, är väl utvecklad och prövad idag. Hur dessa ska användas finns tydligt och klart beskrivet i både gemensam och försvarsgrensvisa doktriner. Tillsammans skapar detta ett väl fungerande koncept som är en naturlig och integrerad del av operationer. IO-cellen, som organisationsform, skapar flexibilitet samtidigt som den kan användas på såväl strategisk- som taktisknivå. Genom att komplettera cellen med ”IO Work Group” säkerställer man synergieffekten av informationsoperationsinsatser sett mot övriga tillgängliga medel. Vald organisationsstruktur underlättar även multinationella insatser där övriga deltagande nationer kan delta med de förmågor dessa medför. För att säkerställa samordningen mellan informationsoperationer och övriga medel i stabsprocesserna, exempelvis vid bekämpning, har man anpassat sig till aktuella tidshorisonter. Man använder även samma typer av tabeller och matriser för planering och genomförande som övriga berörda sektioner.

7.6 Hur ser den svenska Försvarsmakten på informationsoperationer, som metod, över hela konfliktskalan?

Jag har funnit efter studier av skrivit underlag och genomförda intervjuer att det finns en tydlig och relativt gemensam syn på hur informationsoperationer skall användas i Sverige, såväl politiskt som militärt. Informationsoperationer är och skall vara en naturlig och integrerad del i alla typer av operationer. Bristen är hur detta skall ske i praktiken. Gällande principer för myndighetsansvar och lagstiftning utgör en begränsning för tvärsektoriell nationell samordning avseende informationsoperationer.

7.7 Finns det några avgörande skillnader mellan svensk och amerikansk syn på informationsoperationer?

Jag har inte hittat några avgörande skillnader mellan svensk och amerikansk syn. Skillnaderna som finns är mer av semantisk och praktisk art. Den stora, och inte minst naturliga, skillnaden är förmågan att genomföra offensiva informationsoperationer.

7.8 Hur skulle en svensk ledning och planering av informationsoperationer kunna ske vid väpnat angrepp?

Jag har funnit att den mest styrande faktorn för att nå framgång med informationsoperationer är valet av organisation. Ur denna kommer sedan processer och metoder för planering och ledning, vilket sedan säkerställer att den samordning som är nödvändig sker på ett effektivt och rationellt sätt. Svensk anpassning avseende insatsledning till internationell standard gör att det med relativt enkla medel går att redan idag införa en modell för planering och ledning av informationsoperationer inom Försvarsmakten. Denna modell bygger på den amerikanska IO-cellen, med i dag använda processer och metoder, anpassad för svenska förhållanden.

8. Källor och litteratur

Intervjuer

Flottiljamiral Stefan Engdahl	Chef STRA/INRI	2002-03-05
Generalmajor Tony Stigsson	Chef OPL	2002-03-06

Otryckta källor

Försvarsmakten
Underhandsexemplar av *Remiss 1 – Militärstrategisk doktrin* från HKV STRA INRI daterad 2001-06-28, HKV beteckning 19 400:68525

Utlandet
Maj Matt Andersson mfl *Battalion/Task Force Targeting and the Military Decision-Making Process (MDMP) in the Information Operations (IO) Environment*, Mars 2000

Mr Roy W. Hollis *Information Operations Observations, TTP, and Lessons Learned*. November 2001

MCWP 3-40, *Information Operations*, U.S. Marine Corps, Coordinating Draft 2-27-01

MSTP Pamphlet 3-0.4, *Information Operations*, Marine Air Ground Task Force Staff Training Program, U.S. Marine Corps, juli 2000

NATO, *Guidelines For Operational Planning (GOP)*, 1999

NATO, Allied Joint Publication 3.4.1 *Peace Support Operations,* 4th study draft

Newsletter No. 99-2, *Task Force Eagle Information Operations "IO in a Peace Enforcement Environment"*, Center For Army Lessons Learned (CALL) Fort Leavenworth Kansas, USA januari 1999

Schneider and Lawrence, *Battlefield of the Future –21st Century Warfare Issues*, Air War College Studies in National Security No. 3, USA

Maj Arthur Tulak *The Physical Destruction Component of Information Operations in Peace Enforcement*, oktober 1998 och *PSYOP C2W Information Operations in Bosnia,* juni 1999

Övriga handlingar
Dearth Douglas H. Anteckningar och bildspel föreläsning *Conflict in the Information Age: Re-Thinking the Application of Power in the 21st Century* vid FHS den 30 maj 2001

Frykholm Anders, *Informationsoperationer – en möjlighet för Sverige?*, Enskild uppsats, 19100:6021, 2000

HKV STRA/INRI bildspel avseende *Försvarsmakten och Informationsoperationer* samt minnesanteckningar från STRA/INRI toppmöte IO 2001-12-11.

Klingvall Per, *Informationsoperationer vid fredsfrämjande insatser – svensk förmåga eller oförmåga?* C-uppsats, 19100:1002, 2001

Kurkiewicz Ulf, *Informationsteknologins inverkan på svensk försvarspolitik,* Enskild uppsats, 19100:6010, 2000

Rapport nr 1 från arbetsgruppen om informationskrigföring*, Åtgärder och skydd mot informationskrigföring* Stockholm 1997-08-15

Rapport nr 2 (öppen) från arbetsgruppen om informationskrigföring, *Åtgärder och skydd mot informationskrigföring – förslag till ansvarsfördelning m.m.* Stockholm 1998-08-19

Wik Manuel W. Bildspel föreläsning Informationsoperationer – En strategi för fred Informationskrigföring – En avgörande spjutspets i krig vid FHS den 10 april 1999

Internet

Center for Army Lessons Learned (CALL), US Army, *Hot topics Information Operations* *http://call.army.mil/call.html,* 2001-11-06

MoD UK *Lessons Learned from Kosovo*, *http://www.mod.uk/index.php3?page=1542*, 2001-11-06

Annex A till *Lessons from the Crisis*, Ministry of Defence UK, *http://www.mod.uk/index.php3?page=1540* , 2001-11-08

USMC Doctrine Division the Doctrine Publication Hierarchy, *http://www.doctrine.quantico.usmc.mil/* , 2001-07-02

Tryckta källor

Regeringen

Regering *Gränsöverskridande sårbarhet – Gemensam säkerhet Ds2001:14* 2001-03-02

Regeringens proposition 2001/02:10 *Fortsatt förnyelse av totalförsvaret*, Stockholm september 2001

Regeringens proposition 2001/02:158 *Samhällets säkerhet och beredskap*, Stockholm mars 2002

Regleringsbrevet för budgetåret 2002 avseende Försvarsmakten, Stockholm december 2001

Försvarsmakten och Försvarshögskolan
HKV PLANS STRAT, *Försvarsmaktidé 2020 Rapport 3*, daterad 1999-05-19, HKV beteckning 23 210:65117

HKV STRAT, *Försvarsmaktsidé och målbild Rapport 4*, daterad 2000-03-01 HKV beteckning 23 210:61977

HKV STRA UTV, *Försvarsmaktsidé och målbild Rapport 5*, daterad 2001-02-26 HKV beteckning 23 210:62144

HKV STRA UTV*, Årsrapport från perspektivplaneringen 2001-2002; Idébilder och fördjupningsområden inför Försvarsbeslut 2004 – rapport 6* . HKV beteckning 23 210:62 285

Försvarsmakten, *Joint Military Doctrine – Peace Support Operations*, MSK ToD Stockholm 1997

Försvarsmakten 2001, *Försvarsmaktens grundsyn ledning – FM Grundsyn Ledning,* Tryck och produktion; MSK, Stockholm 2001

Utlandet
Joint Pub 3-13, *Joint Doctrine for Information Operations*, US Defence Forces, den 9 oktober 1998

Böcker
Bowden Mark, *Black Hawk Down*, Bantam Press, Chatham Kent, Storbritannien 1999

Kingdon John W, *Agendas, Alternatives, and Public Policies,* Second Edition HarperCollins College Publishers, USA 1995

Van Creveld Martin, *Command in War*, Harvard University Press Cambridge, USA 1985

Starrin mfl *Från upptäckt till presentation*, Studentlitteratur ISBN 91-44-32121-X, Sverige 2000

Litteratur

Campen, Dearth, *Cyberwar 2.0: Myths, Mysteries and Reality* AFCEA International Press (AIP), Fairfax Virginia USA, Juni 1998

Campen, Dearth, *Cyberwar3.0: Human Factors in Information Operations and Future Conflict* AFCEA International Press (AIP), Fairfax Virginia USA, Oktober 2000

Bilaga 1 Abstract

A Swedish model for Information operations

This essay explores and develops a Swedish model for information operations, concerning C2 and planning, which will work both in national defence as well as when participating in multinational crisis response operations.

The purpose of the essay is to bring knowledge about where Sweden stands today concerning its view on information operations, and develop a model for C2 and planning that suits the Swedish Defence Forces.

The essay uses a developed qualitative method with a qualitative analysis of documents and interviews. The scientific procedure used includes analyse, fact collection, a process of qualitative comparison and finally a synthesis.

The essay describes the current American and Swedish view on information operations. Compares if there are any deciding differences between the views and after this a hypothesis is tested. This testing results in a model for Swedish C2 and planning of information operations. This model is finally exemplified by using a scenario of a military operation for national defence.

Keywords: Information operations, American view, a Swedish model, C2 and planning, national defence.

Bilaga 2 Förkortningar och nyckelbegrepp

Följande definitioner och förklaringar är hämtade, om inget särskilt anges, från underbilaga 1 till skrivelsen 23 210:62 285, *, Årsrapport från perspektivplaneringen 2001-2002; Idébilder och fördjupningsområden inför Försvarsbeslut 2004 – rapport 6* .

Asymmetrisk krigföring - Under senare år har begreppet asymmetrisk krigföring kommit att användas i olika sammanhang. Asymmetrisk krigföring som begrepp, har i USA utnyttjats för att beskriva bland annat terrormetoder mot det amerikanska samhället. Syftet har varit att särskilt uppmärksamma risken för denna av typ angrepp.

Asymmetri är ett tillstånd som uppstår när två förhållanden som är olika varandra möts. Det är olikheten som är asymmetrin, inte metoderna i sig. Det är först i mötet mellan angreppsmetoderna och försvarsansträngningarna som det går att avgöra om det uppstått en asymmetri. Begreppet beskriver en avsikt att undvika att möta en motståndare där han är stark utan istället agera mot hans svaga sidor. Ofta används metoder som avsevärt skiljer sig från vad som förväntas. Exempelvis kan metoderna baseras på olika vilja att uthärda förluster bland underställda och tredje part, eller olika beredvillighet att åsidosätta folkrätt och annan internationell lagstiftning.

Asymmetrisk krigföring kan utnyttjas av såväl statliga, som icke-statliga aktörer, och riktas såväl mot motståndarens militära styrkor som dess samhälle. Asymmetrisk krigföring kan innehålla exempelvis terrorism, massförstörelsevapen och informationskrigföring.

Informationsoperationer (IO) - Riktade och samordnade åtgärder till stöd för egna politiska och/eller militära mål genom att påverka eller utnyttja motståndarens eller annan utländsk aktörs information och/eller informationssystem. Det yttersta målet är att påverka det mänskliga beslutsfattandet. IO kan genomföras i såväl politiska, ekonomiska som militära sammanhang.

Defensiva informationsoperationer (IO-D) - Riktade och vanligen samordnade åtgärder i fred, kris och krig avseende operationer, personal, teknologi och policy för att skydda och försvara information, informationssystem och egen förmåga till rationellt beslutsfattande. Genomförs t.ex. genom fysiskt skydd, skydd mot vilseledning, skydd mot informationsinhämtning, säkerhetsunderrättelsetjänst och telekrigsåtgärder och psykologiskt försvar.

Offensiva informationsoperationer (IO-O) - Riktade och vanligen samordnade åtgärder i fred, kris och krig för att påverka en motståndares information och/eller informations- och kommunikationssystem. Målet är bland annat att påverka dennes förmåga till rationellt beslutsfattande och därmed gynna egna syften. Genomförs t.ex. genom fysisk attack/förstöring, vilseledning, skydd mot informationsinhämtning, telekrig och psykologiska operationer.

Informationskrigföring - Informationsoperation som genomförs under kris och krig för att främja eller uppnå särskilda politiska och/eller militära mål gentemot en eller flera motståndare.

Informationsöverlägsenhet - Med informationsöverlägsenhet menas att ha bättre omvärldsuppfattning än motståndaren. Förutsättningarna för att uppnå detta är att ha bättre ledning, bättre uppföljning av egna stridskrafter och bättre underrättelsetjänst än motståndaren samt förmåga att begränsa motståndarens omvärldsuppfattning genom ledningskrigföring.

Kris - Politisk händelseutveckling och/eller naturkatastrofer med militära och/eller samhälleliga följdverkningar. Kriser i närområdet sammankopplas med beredskapshöjningar.

Ledningskrigföring - Militär verksamhet som syftar till att försämra motståndarens eller annan aktörs omvärldsuppfattning och nedsätta förmågan att utöva ledning. Består av ledningsbekämpning, vilseledning, psykologiska operationer och skydd mot informationsinhämtning.

Ny krigföring - Svenskt begrepp synonymt med RMA. D.v.s. att med teknikens hjälp skapa bättre balans mellan informations- lednings- och verkanssystem.

Nätverksbaserat försvar - En struktur innehållande ledning med beslutsstöd, informationssystem samt insats- och verkansfunktioner. Dessa är integrerade med varandra och medger informationsutbyte i nära realtid.

Operation - Militär insats utförd av förband ur grund- eller insatsorganisationen på strategisk, operativ eller taktisk nivå. Jfr NATO:s ”operation”.

Gemensam operation - Militär insats utförd av förband ur flera försvarsgrenar ur grund- eller insatsorganisationen. Gemensam operation leds under ÖB av C OPIL. Jfr NATO:s ”Joint operation”.

Psykologisk krigföring - Åtgärder som en stat eller en grupp av stater vidtar för att försvaga försvarsvilja och motståndsanda hos befolkningen i en annan stat eller grupp av stater. Verksamhet som syftar till att påverka opinioner, känslor, åsikter och uppträdande på ett för våra avsikter gynnsamt sätt.

Bilaga 3 Frågeställningar vid intervju

Bakgrund

Mitt syfte med uppsatsen är att, med hjälp av en explorativ studie, skapa en tes i form av en generell modell avseende svensk ledning och planering av informationsoperationer. Inom ramen för uppsatsen kommer jag att undersöka hur svensk ledning och planering av informationsoperationer, för såväl nationell som internationell insats kan genomföras. För att nå dit kommer jag att använda följande huvudfrågeställningar;

- Hur ser den amerikanska doktrinen för informationsoperationer ut?
- Hur ser den svenska Försvarsmakten på informationsoperationer, som metod, över hela konfliktskalan?
- Finns det några avgörande skillnader mellan svensk och amerikansk syn på informationsoperationer?
- Hur skulle svensk planering och ledning av informationsoperationer kunna ske vid försvar mot väpnat angrepp?

Syftet med intervjun är dels att undersöka vilken syn nyckelpersoner inom Försvarsmakten har på informationsoperationer främst ur perspektivet ledning och planering, men även utgöra en form av källkritisk granskning.

Frågor

1. Är informationsoperationer något nytt och tidigare outforskat område inom svenska Försvarsmakten?
2. Ser ni någon/några gränssättande faktor/er för nyttjandet av informationsoperationer för Försvarsmakten?
3. Ser ni någon principiell skillnaden avseende nyttjandet av informationsoperationer beroende på vilken huvuduppgift man löser?
4. Delar ni uppfattningen att informationsoperationer/informationskrigföring har en potential som jämställer den med mark-, sjö- och luftkrigföring på det moderna slagfältet och nätverkscentrerad krigföring? (Denna innebörd uttalas i utkastet till militärstrategisk doktrin)
5. Ser ni någon orsak eller annan begränsande faktor som gör att Försvarsmakten inte kan nyttja samma övergripande procedurer och metoder i ledning och planering som NATO?
6. Hur ser ni på rollspelet mellan militärstrategisk och operativ nivå vad gäller ledning och planering av informationsoperationer?
7. Hur ser ni på ledning och planering av informationsoperationer i förhållande till ledning med uppdragstaktik, centraliserad och decentraliserad ledning?
8. Vilken nivå tycker ni är den lägsta där man kan nyttja informationsoperationer?
9. Vilken väg ser ni för framtagandet av en svensk modell för ledning och planering av informationsoperationer?
10. Uppfattar ni att regeringen prioriterar eller har ett särskilt intresse för informationsoperationer?